silex technology

SX-500-1402

Serial Device Server

Cryptographic Officer Guidance Manual

Part Number 140-00188-210A

June2009

Silex Technology America SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS OF THIS PRODUCT FOR A PARTICULAR PURPOSE. Silex shall not be liable for any errors contained in this manual or for any damages resulting from loss of use, data, profits, or any incidental or consequential damages arising from the use of SILEX products or services. The information contained in this documentation is subject to change without notice.

The firmware embedded in this SX-500 serial device server includes the eCos operating system. eCos and certain other software programs used in the SX-500 are licensed under GNU GPL compatible Free Software Licenses (with the eCos exception clause). In compliance with these licenses, you can obtain the relevant source code at no charge by contacting Silex at support@silexamerica.com.

Trademarks

All company or product names referenced in this document may be trademarks or registered trademarks of their respective owners.

Silex Technology America, Inc.

www.silexamerica.com

Part Number 140-00188-210A

Contents

Figures

Tables

About This Reference Guide

Safety Precautions

- To prevent damage to the Serial Device Server’s electronic circuit components, follow established ESD practices and procedures for handling static-sensitive devices. All ESD-sensitive components must be stored and shipped in ESD-conductive bags or bubble-wrap and labeled as such using the standardized ESD adhesive warning label.
- Ethernet electrical wiring must be at least 6 feet from bare power wiring or lightning rods and associated wires, and at least 6 inches from other types of wire (antenna wires, doorbell wires, wires from transformers to neon signs), steam or hot water pipes, and heating devices.
- Protectors and grounding wire placed by the service provider must not be connected to, removed, or modified by the customer.

Emissions Disclaimer

Regulatory compliance information can be found in Appendix D of this manual. Final emission certification per FCC, CE and other agency requirements are the responsibility of the OEM using any printed circuit assemblies or other items used in this developer’s kit in their saleable packaged product.

REVISION HISTORY

Rev. No.	Date	Revision by	Comments
A	2009.08.13	Lee Aydelotte	Initial Release

Chapter 1: Introduction

The SX-500-1402 Serial Device Server provides a FIPS 140 compliant encrypted wireless LAN connection for an attached client device. The client device may attach to the SX-500 via a serial port or wired Ethernet port.

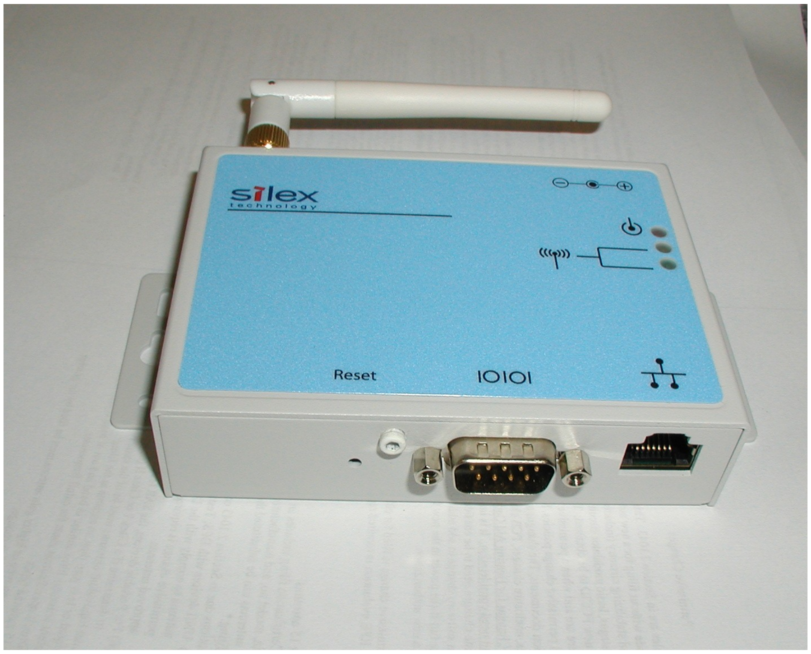


Figure 1 SX-500

PHYSICAL PORTS

The physical ports on the SX-500 are as follows:

Port Name	Description
Power	Jack for attachment of external power supply
Ethernet	RJ-45 connector for attachment of Ethernet cable
Serial	DB-9 connector for attachment of serial interface cable
Wireless	RP-SMA connector for attachment of an external antenna
Button	Momentary push button
LED	Green, Yellow and Orange LEDs

For installation and connection of the interface ports, refer to Chapter 2.

Logical Ports

The SX-500 has logical interfaces for transfer of data and for configuration and control of the unit. These logical interfaces may share a physical port. The application firmware in the SX-500 separates and routes the data to the appropriate internal firmware task associated with the logical interface. For network ports (Ethernet, Wireless) this separation is based on the TCP or UDP protocol port number. For the serial port, data or control/status mode is controlled by specific protocol strings, only one mode is active at a time. Serial port control/status mode is only available if the unit is explicitly configured to allow it. The following table describes the logical interfaces of the unit when operating in a FIPS 140-2 approved mode.

FIPS-140-2 Interface	Physical Interface	Logical Interface
Data Input	Serial	Plaintext data for transmission to network
	Ethernet	Plaintext data for bridging to wireless network
	Wireless	Ciphertext data for Serial or Ethernet port
Data Output	Serial	Plaintext data received from wireless network
	Ethernet	Plaintext data received from wireless network
	Wireless	Ciphertext data from Serial or Ethernet port
Control Input	Ethernet	Control data for console task received via Telnet
		Control data for web config task received via HTTP
	Wireless	Control data for console task received via Telnet
		Control data for web config task received via HTTP

FIPS-140-2 Interface	Physical Interface	Logical Interface
	Button	Invoke configuration/status function
Status Output	Ethernet	Plaintext status response from console task via Telnet
		Plaintext status response from web config via HTTP
	Wireless	Status response from console task via Telnet
		Status response from web config via HTTP
	Serial	Plaintext status response from button push
	LEDs	Indicate link and unit error status
Power Interface	Power	
	Serial	

When the module enters an error state, all Data Input and Data Output interfaces are disabled. If an error state is encountered, the LED interface will indicate the error by blinking for several seconds, and then the unit will reset. The unit will not send or receive any data until the reset is complete.

The SX-500 performs cryptographic self tests during initialization after power up or a firmware induced reset. Until the self tests are complete, no data input or output interfaces are active. If the self test fails, the unit will enter an error state.

Configuration

The Cryptographic Officer is responsible for configuring the unit for use in the target environment. See Chapter 3 and Appendix A for instructions on configuring the unit. The peripheral unit (usually a PC) being used to configure the SX-500 must be directly connected to the unit via a crossover cable or local hub which is not connected to any LAN, WLAN or other larger network. This will enable manual transport and electronic entry of secret and private keys (RSA private key and WPA Pre-Shared Key) in a plaintext form. Even if RSA private keys are protected with a PEM passphrase when entered, they are still considered to be in plaintext form.

For the SX-500 to operate in FIPS 140-2 approved mode, the wireless security configuration must be set as follows:

Item	Required Setting
Wireless Encryption Mode	WPA2 (AES-CCMP)
Wireless Authentication	PSK or TLS or PEAP

The SX-500 allows other security settings for interoperability in non FIPS 140 environments. However, use of the SX-500 with any settings other than those indicated above is not FIPS 140-2 compliant.

In particular, the WPA2-WPA transition mode is NOT FIPS 140-2 compliant. Only networks exclusively using WPA2 (AES-CCMP) encryption comply.

The current security settings for the device may be observed by logging into the unit web server and navigating to the network security page, which will show the currently active and configured values for the above parameters (and others). The settings may also be observed with the configuration console command SHOW NW. This should be done after configuration and before use to verify that the device is properly configured for the intended target environment.

The SX-500 is validated at level 1, which means it has no physical security beyond the physical protection of its metal case, and is presumed to be used in a secure environment. If the unit is to be left unused in an unsecured area, or is to be transported to a new location via unsupervised means, it is recommended that the Cryptographic Officer zeroize the device. This is done with the configuration console command ZEROKEYS. After zeroization the unit will need to be re-configured before wireless communication in FIPS compliant mode are possible.

The Cryptographic Officer must be aware that all configuration program inputs are in plaintext for purposes of FIPS 140-2 compliance regardless of the transport encoding used. The only FIPS 140-2 cryptographic protection claimed for this module is for the wireless link between the unit and an associated Access Point.

If WPA2-PSK mode is being used, the PSK must be entered by the Cryptographic officer on an isolated network with the machine containing Cryptographic Officer's web browser directly connected to the SX-500 and not connected via a LAN. The same is true for entry of externally generated RSA private keys/public certificates.

The Crypographic officer must zeroize the module when transitioning the device configuration from a FIPS-140-2 approved mode to a non-approved mode. The Cryptographic Officer should zeroize the module before resetting the configuration to factory defaults. If this is impossible, because the reason for resetting is the connection to the unit is impossible, the unit must be zeroized after the configuration reset is complete and connection has been restored.

There are two types of bypass states possible with the module (non-approved modes). The first is to use any wireless encryption/authentication combination not specified above as being FIPS 140-2 compliant and then reset the unit. The second is to configure the unit to not be in Ethernet to Wireless mode, plug in a wired Ethernet cable, and then reset the unit.

If WPA2-PSK mode is being used, the PSK must be entered by the Cryptographic officer on an isolated network with the machine containing Cryptographic Officer's web browser directly connected to the SX-500 and not connected via a LAN. The same is true for entry of externally generated RSA private keys/public certificates.

In addition to the wireless security settings above, the following settings must be made for operation in FIPS 140-2 mode:

Item	**Required Setting**
HTTPS	Disabled (factory default)
S-Telnet	Disabled (factory default)
TCP data service SSL	Disabled (factory default)
Serial port console mode string	NULL (disabled – factory default)
Serial port filter	TRAP (factory default)

Physical Protection

There are no user serviceable parts inside the SX-500 enclosure. If the enclosure should be opened for any reason, the Cryptographic Officer should zeorize the module before the enclosure is opened.

Secure Operation

The Cryptographic Officer and any users of the SX-500 module must be familiar with the SX-500 Cryptographic Security Policy and must follow its guidelines for proper operation.

Chapter 2
Installing the Serial Device Server Hardware

The Serial Device Server includes most of the hardware and software components required for installation. The one item that you will need to purchase separately is a cable to connect your serial device to the Serial Device Server (this cable is not included because of the wide variety of connector types used on serial devices).

Verify Package Contents

The Serial Device Server includes the components listed in Table 1. Please ensure that all materials listed are present and free from visible damage or defects before proceeding. If anything appears to be missing or damaged, please contact Silex.

Table 1 Package Contents

Description
SX-500 Base Unit w/external pole antenna
Setup Guide
CD-ROM containing Serial Port Emulator Software, and User's Reference Guide
AC Power Supply with power cord
Warranty Card

Installing the Serial Device Server

Follow the steps below to install the Serial Device Server. The Serial Device Server's factory default settings should be sufficient for most serial connections; however, some of the configuration settings may have to be changed for your particular installation.

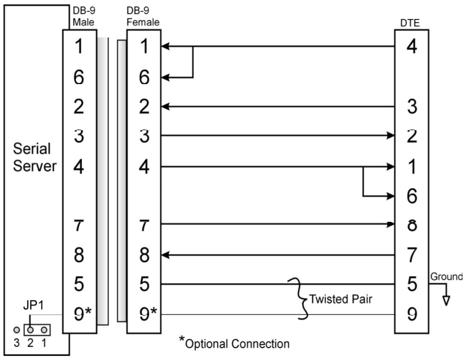
1. Before attempting to install the Serial Device Server, make sure you have installed and set up your serial device as described in the documentation that came with the device.

2. Write down the 12-digit MAC (Media Access Code) address printed on the label located on the bottom of the Serial Device Server (for example: 004017023F96). You may need this number in order to configure the Serial Device Server.

3. If you have a wireless model, connect the antenna to the unit.

4. Connect the Serial Device Server to your serial device. If you are using RS-232, you may use standard PC cabling (you should normally use a null modem crossover cable). The 9-pin connector pinouts and cabling are as follows:

Pin	Description
1	DCD (Data Carrier Detect) Input
6	DSR (Data Set Ready) Input
2	RxD (Receive Data) Input
3	TxD (Transmit Data) Output
4	DTR (Data Terminal Ready) Output
7	RTS (Request To Send) Output
8	CTS (Clear To Send) Input
5	Ground
9	RI (Ring) Input or +5 VDC Power Input (Optional)



RS-232 connector pinouts and cabling

5. Plug the Serial Device Server power supply adapter into a suitable AC receptacle, and then plug the power supply cable into the Serial Device Server. Alternatively, you can use pin 9 on the 9-pin connector to provide power to the Serial Device Server (1 amp @ +5V is required).

   When power is applied all three LEDs will be lit. The Serial Device Server will run through a sequence of power-up diagnostics for a few seconds.

- If the Serial Device Server is operating properly, the green and yellow LEDs will turn off and then will show the device status as shown in Table 2 in the next section. The orange LED should remain solidly illuminated.
- The unit powers up in the Normal mode, which provides for connection from the network to device(s) connected to the serial port of the Serial Device Server.
- If the orange LED blinks continuously in a regular pattern, a problem exists. If this is the case, try powering the unit OFF and then ON again.

NOTE: Pin 9 is normally configured for supplying +5V from an external power source in lieu of using the AC power supply adapter.

6. Connect the Serial Device Server to your network through a switch or hub using a category 5 (CAT5) Ethernet cable. Then cycle power on the device to switch the server into wired mode and switch off the wireless networking functionality as long as the cable is plugged in.

NOTE: SILEX RECOMMENDS USING A HARDWIRED ETHERNET CONNECTION FOR CONFIGURING WIRELESS SERIAL DEVICE SERVERS. If you have a wireless Serial Device Server model and cannot use an Ethernet connection, refer to step 4 in the *First Time IP Address Configuration* section of this chapter for instructions on how to set up the Serial Device Server using a completely wireless Ad Hoc environment. Device Keys (unit private key and WPA2-PSK) must be entered via an isolated wired connection

7. The Serial Device Server's IP address must be configured before a network connection is available. If your network offers DHCP (Dynamic Host Configuration Protocol), the Serial Device Server will automatically search for a DCHP server upon power up and obtain an IP address. If your network does not offer DHCP, a static (fixed) IP address must be assigned (see your system administrator for assistance). If you use DHCP, make sure that the length of the DHCP lease is adequate so that the IP address of the Serial Device Server does not change.

Monitoring Serial Device Server Status

You can monitor the Serial Device Server status using the yellow, green and orange LED status indicators on the monitor. Table 2 defines the functions of the LED status indicators.

Table 2 Status Monitors

Function	State	Status
Power Orange	On	The Serial Device Server is receiving power
	Off	The Serial Device Server is not receiving power
	Slow Blink (0.6Hz)	Firmware update in progress
	Fast Blink (5-10Hz)	The Serial Device Server is malfunctioning or cryptographic error detected.
Network Status Yellow or Green	Yellow Off Green Off	No network connection
	Yellow On Green Off	Wireless network connected, not authenticated.
	Yellow On Green On	Wireless network active (authenticated) in FIPS 140-2 approved mode.
	Yellow Blinking (5Hz) Green On	Wireless network data received in FIPS 140-2 approved mode.
	Yellow off Green Blinking (½ Hz)	Bypass (non-approved) mode, no wireless network connection
	Yellow on Green Blinking (½ Hz)	Bypass mode, wireless network connected.
	Yellow Blinking (5 Hz) Green Blinking (5 Hz)	Bypass mode, wireless network data received

Chapter 3
Configuring the Serial Device Server

This chapter describes the methods for configuring the basic settings of the Serial Device Server, including the IP address, serial port settings, and wireless security. The Serial Device Server also has an extensive range of advanced configuration capabilities that are described in Chapter 5, Appendix A, and Appendix B. The Serial Device Server configuration should be done by a network administrator or another person with technical knowledge of TCP/IP networking and serial communications.

Basic Configuration Requirements

In order to use the Serial Device Server, the following basic parameters must be configured:

TCP/IP Settings:

- IP Address
- Subnet Mask
- Router Address

Note: The TCP/IP settings can be automatically configured using DHCP.

Wireless Configuration Settings:

- SSID
- Mode (Infrastructure or Ad Hoc)
- Channel (required only if using Ad Hoc mode)

Security Settings:

- Wireless Encryption Mode (WPA2, WPA, WPA2-WPA, WEP)
- Wireless Encryption Settings
- Wireless Authentication Mode (WPA-PSK, Open System, Shared Key, TTLS, TLS, LEAP, PEAP)
- Wired Authentication Mode (TTLS, TLS, PEAP)
- Authentication Settings

Note: There are numerous possible encryption and authentication settings, and every network can have different settings. Please refer to Appendix A for a detailed summary of these settings.

Serial Port Settings (must match the settings of the attached serial device):

- Baud Rate (Speed)
- Parity
- Character Size

- Flow Control

In addition to the above parameters, the Serial Device Server allows you to configure numerous other capabilities. These other capabilities provide you with the unparalleled flexibility to use the Serial Device Server on virtually any 802.11 or Ethernet network with a wide range of serial devices.

Configuration Methods

There are two ways to configure the Serial Device Server:

- *Internal Web Pages (HTTP).* You can use any standard web browser to access the Serial Device Server internal web pages. These web pages provide an easy-to-use graphical interface for configuring the Serial Device Server. In order to use the internal web pages for the first time, you must assign the Serial Device Server IP address using some other method (for example, DHCP or arp/ping). This initial IP address assignment need only be done one time.

- *Internal Command Console.* The internal command console provides a sophisticated command line interface for advanced users to configure the Serial Device Server. It can be accessed by connecting a serial cable to the serial port and using console mode switching as descried in chapter 4. Once the IP address has been assigned, the internal command console can also be accessed via TELNET, or via the internal web pages. NOTE: when operating in a FIPS 140-2 approved mode, the console is not available via the serial port.

If you have a Serial Device Server wireless model, Silex recommends that you temporarily plug the Serial Device into a wired Ethernet network during the configuration process. Although it is possible to configure the Serial Device Server with a completely wireless setup, it is much simpler to perform the process using a wired Ethernet connection. This is primarily because the wireless security on most wireless networks prevents the addition of a new wireless device unless all security parameters are first entered into that device. As a result, you must set up a temporary dedicated ad hoc wireless network in order to configure the Serial Device Server in a completely wireless environment (refer to the step 4 in the *First Time IP Address Configuration* section of this chapter for instructions on how to set up the Serial Device Server using a completely wireless Ad Hoc environment). **This is required when entering security encryption keys (RSA private key or WPA2-PSK).**

Configuring the Serial Device Server using each of the above methods is described in the following sections of this chapter.

First-Time IP Address Configuration

NOTE: Skip this section if you have already configured the SX-500 IP address

If you are configuring the Serial Device Server from a non-Windows computer or if you cannot use an Ethernet connection, you must first configure the Serial Device Server IP address. Note that it is only necessary to perform this task one time -- once the address has been configured, the Serial Device Server can be accessed from any computer on the network that has the appropriate privileges. The steps are as follows:

1. If your network has a DHCP server and you can use an Ethernet connection to the Serial Device Server:

   a. Make sure your PC is connected and has access to your network.

   b. Connect an Ethernet cable from your network hub to the Serial Device Server (if you have a wireless Serial Device Server and do not have hardwired capabilities, then you must go to Step 4 below for setup instructions).

   c. Power on the Serial Device Server.

   d. The administration program on most DHCP servers logs the IP address and MAC address of each DHCP client. The MAC address of the Serial Device Server can be found on the label affixed to the unit. If your DHCP server has logged this information, write down the IP address of the Serial Device Server for future reference. You are now ready to configure the Serial Device Server (skip the remainder of this section).

   e. If your DHCP server does not provide client information or if you do not have access to the DHCP server, then you can get the IP address by connecting a serial device such as a printer, a Windows PC running HyperTerminal, or another serial device capable of printing ASCII characters to the serial port the Serial Device Server). Your serial device must be set at 115.2Kbps, 8-bit character size, and no parity.

   f. With the serial device and Serial Device Server switched on and ready, press the ***Reset*** pushbutton on the Serial Device Server. This will cause the Serial Device Server configuration data to be sent to the connected serial device. The serial device should display or print the current IP address assigned to the Serial Device Server by your network DHCP service. Write down this address for future reference. You are now ready to configure the Serial Device Server (skip the remainder of this section).

2. If you can connect the Serial Device Server via Ethernet but do not have a DHCP server, then you must use the following procedure for the first-time IP configuration of the Serial Device Server.

   a. Make sure your PC is connected and has access to your network

   b. Connect an Ethernet cable from your network hub to the Serial Device Server. The Serial Device Server must be on the same network segment as the PC (that is, there can be no router between the Serial Device Server and the PC).

   c. From the Windows Command Prompt (MS-DOS Prompt), the Mac OS X Terminal Utility, or the UNIX/Linux command line, enter the command

```
arp –s ipaddress macaddress
```

```
ping ipaddress
```

Where *ipaddress* is the desired IP address of the Serial Device Server and *macaddress* is the MAC address of the Serial Device Server (found on the label affixed to the Serial Device Server). For example:

```
arp –s 192.168.5.53 00:40:17:00:00:01

ping 192.168.5.53
```

Note that Windows systems use the format *xx-xx-xx-xx-xx-x*x for the MAC address (for example, 00-0017-00-00-01).

You will see a reply from the Serial Device Server with the number of bytes and other information if the address was successfully set.

If you get an error message or no response, then the IP address was not set. If this is the case, the Serial Device Server may not be at its default configuration. To reset the Serial Device Server to its default settings, hold down the reset pushbutton for more than five seconds.

d. You are now ready to configure the Serial Device Server (skip the remainder of this section).

NOTE: Skip the following step if you have configured IP address of the Serial Device Server using an Ethernet cable.

3. If you are using a wireless connection for the first-time configuration of the Serial Device Server, you must set up a temporary ad hoc wireless connection as described in the following steps. Please note that because this is a fairly complex process, we do not recommend it unless it is not possible to use a wired connection.

a. Disconnect your PC and the Serial Device Server from your network, and temporarily set the PC settings as follows:

- IP address: 192.0.0.191
- Wireless Mode: ***Ad Hoc*** (sometimes referred to as Peer-to-Peer)
- Channel: ***11***
- SSID (or wireless network name): ***serserv***

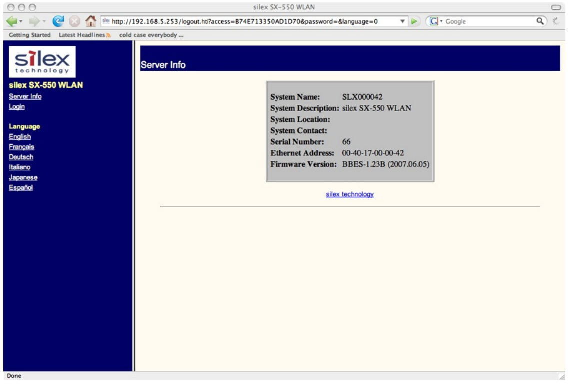
b. Power on the PC and the Serial Device Server. You can connect to the Serial Device Server by specifying its default IP address of 192.0.0.192 using a web browser as described in the next section. When you have connected to the Serial Device Server, you must then change the IP address and enter the required wireless networking parameters using either the web browser interface or the internal command console (see next two sections) for operation on your wireless network.

c. After you complete the entire Serial Device Server configuration process, you must set your PC back to its original network settings.

Using a Web Browser to Configure the Serial Device Server

After you have entered an IP address into the Serial Device Server, you can use any standard web browser to access the internal web pages for configuring the Serial Device Server. Simply specify the IP address of the Serial Device Server in your browser and then follow the steps below:

<u>IMPORTANT</u>: You must click the *Submit button* when you have finished configuring an internal web page. If you do not do this, your changes will not be saved.

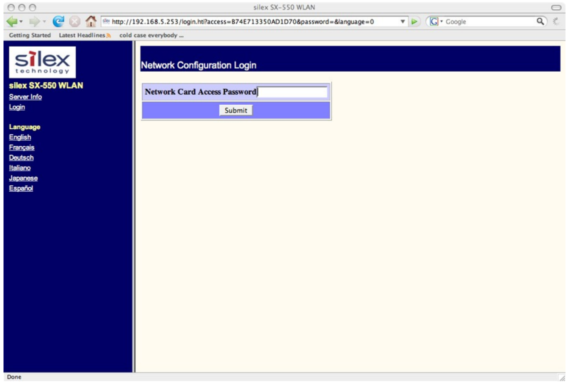


http://192.168.5.253/logout.hti?access=B74E713350AD1D70&password=&language=0

Server Info

System Name: SLX000042
System Description: silex SX-550 WLAN
System Location:
System Contact:
Serial Number: 66
Ethernet Address: 00-40-17-00-00-42
Firmware Version: BBES-1.23B (2007.06.05)

1. When you have connected to the Serial Device Server, you will get the Server Info page. Click ***Login*** on the left side of the screen.

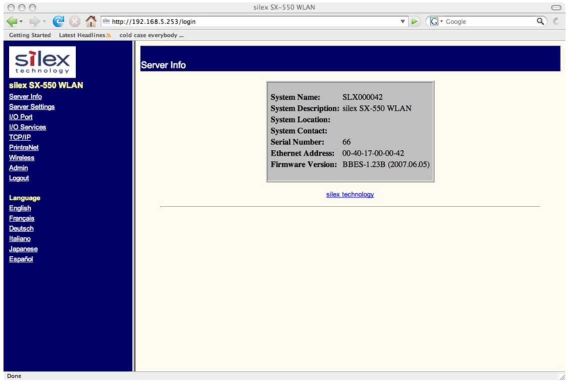


http://192.168.5.253/login.hti?access=B74E713350AD1D70&password=&language=0

Network Configuration Login

Network Card Access Password

2. Enter the password ***access*** and press ***Submit***.

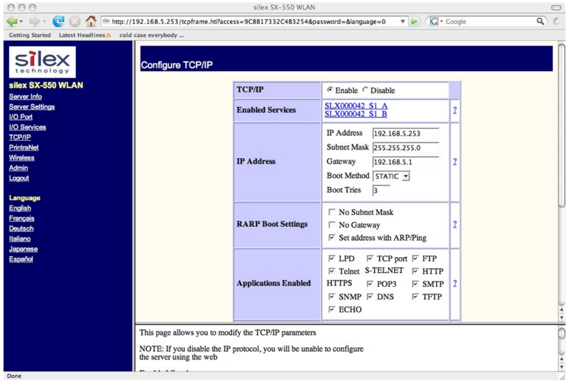


http://192.168.5.253/login

Server Info

System Name: SLX000042
System Description: silex SX-550 WLAN
System Location:
System Contact:
Serial Number: 66
Ethernet Address: 00-40-17-00-00-42
Firmware Version: BBES-1.23B (2007.06.05)

3. You will return to the Server Info page, but new options will be listed on the left side of the screen. Click on ***TCP/IP***.



Configure TCP/IP

TCP/IP	● Enable ○ Disable	
Enabled Services	SLX000042_S1_A SLX000042_S1_B	?
IP Address	IP Address 192.168.5.253 Subnet Mask 255.255.255.0 Gateway 192.168.5.1 Boot Method STATIC Boot Tries 3	?
RARP Boot Settings	□ No Subnet Mask □ No Gateway ☑ Set address with ARP/Ping	?
Applications Enabled	☑ LPD ☑ TCP port ☑ FTP ☑ Telnet S-TELNET ☑ HTTP HTTPS ☑ POP3 ☑ SMTP ☑ SNMP ☑ DNS ☑ TFTP ☑ ECHO	?

This page allows you to modify the TCP/IP parameters

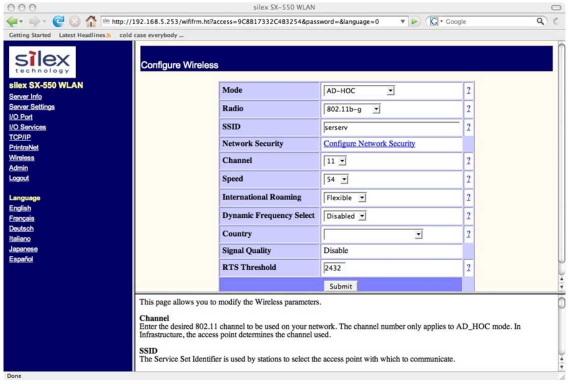
NOTE: If you disable the IP protocol, you will be unable to configure the server using the web

If you used DHCP, verify that the IP address is correctly set. If you used the default 192.0.0.192 IP address, you MUST change it to a new valid IP address. If necessary, change the Subnet Mask and Gateway. It is generally not necessary to change the other parameters on this page (refer to Chapter 5 for advanced configuration information.

Note that on-line help information is available on every configuration page.

Click the ***Submit*** button at the bottom of the window (you may need to scroll) to save your changes.

> **NOTE: If you are using DHCP on your network, the SX-500 should have acquired valid IP settings at this point and no further configuration is necessary. However, for some installations, a static IP address is preferred. If your DHCP server does not allow the SX-500 to keep its assigned IP address permanently, then you must manually assign an IP address. In this case, use a static IP address outside the range reserved for DHCP (see your DHCP server documentation for details). To assign a static IP address, select *Set Permanent* as the *IP Address Resolution*, and assign a valid static IP address for your network. Click on *OK* to save the new settings.**



Configure Wireless

Mode	AD-HOC	?
Radio	802.11b-g	?
SSID	serserv	?
Network Security	Configure Network Security	
Channel	11	?
Speed	54	?
International Roaming	Flexible	?
Dynamic Frequency Select	Disabled	?
Country		?
Signal Quality	Disable	
RTS Threshold	2432	?

This page allows you to modify the Wireless parameters.

Channel
Enter the desired 802.11 channel to be used on your network. The channel number only applies to AD_HOC mode. In Infrastructure, the access point determines the channel used.

SSID
The Service Set Identifier is used by stations to select the access point with which to communicate.

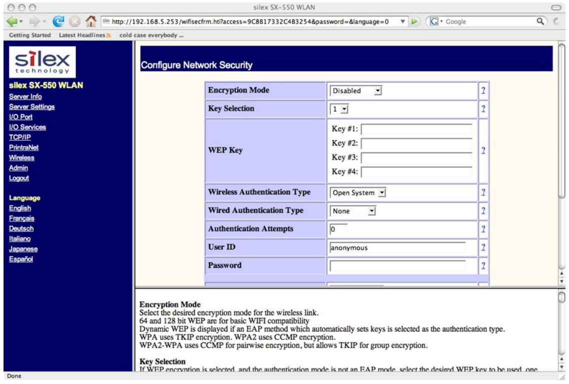
4. Click ***Wireless*** on the left side of the screen to configure the 802.11a/b/g wireless settings (for WLAN models only; skip to the next section if you have an Ethernet model). To operate on an 802.11a/b/g network, the Serial Device Server configuration must be configured with the wireless configuration and security parameters required to allow the Serial Device Server to communicate over your wireless network (check with your network administrator if you do not know these parameters).

    - Select either Infrastructure (if you are using an access point) or Ad Hoc (point-to-point) as the wireless mode
    - Enter the SSID for your network
    - If you are using Ad Hoc, select the RF channel (not required for infrastructure)

    The other parameters on this page do not normally need to be changed (refer to Chapter 5 for information on advanced configuration).

    Click the ***Submit*** button at the bottom of the window (you may need to scroll) to save your changes.

    Now click ***Configure Network Security*** to configure the wireless security parameters.



Configure Network Security

Encryption Mode	Disabled	?
Key Selection	1	?
WEP Key	Key #1: Key #2: Key #3: Key #4:	?
Wireless Authentication Type	Open System	?
Wired Authentication Type	None	?
Authentication Attempts	0	?
User ID	anonymous	?
Password		?

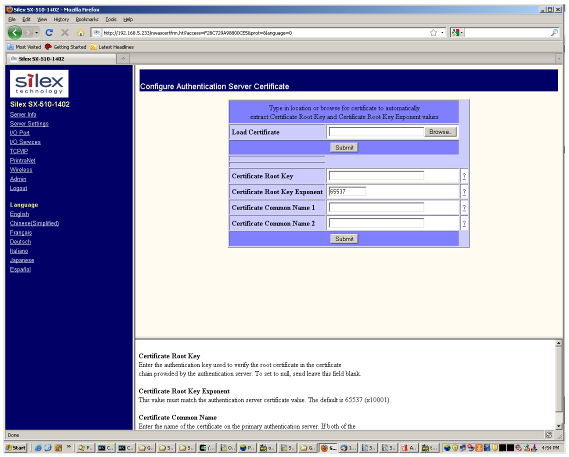
Encryption Mode
Select the desired encryption mode for the wireless link.
64 and 128 bit WEP are for basic WIFI compatibility
Dynamic WEP is displayed if an EAP method which automatically sets keys is selected as the authentication type.
WPA uses TKIP encryption. WPA2 uses CCMP encryption.
WPA2-WPA uses CCMP for pairwise encryption, but allows TKIP for group encryption.

Key Selection
If WEP encryption is selected, and the authentication mode is not an EAP mode, select the desired WEP key to be used, one

5. Select the appropriate wireless encryption mode and enter the required settings (check with your network administrator for the proper settings if you do not know them). Appendix A lists the possible encryption settings.

Click the ***Submit*** button at the bottom of the window (you may need to scroll) to save your changes.

To enter the Authentication Server root signing certifcate, click on ***Configure Authentication Server Certificate***



Configure Authentication Server Certificate

Type in location or browse for certificate to automatically extract Certificate Root Key and Certificate Root Key Exponent values

Load Certificate		
Certificate Root Key		?
Certificate Root Key Exponent	65537	?
Certificate Common Name 1		?
Certificate Common Name 2		?

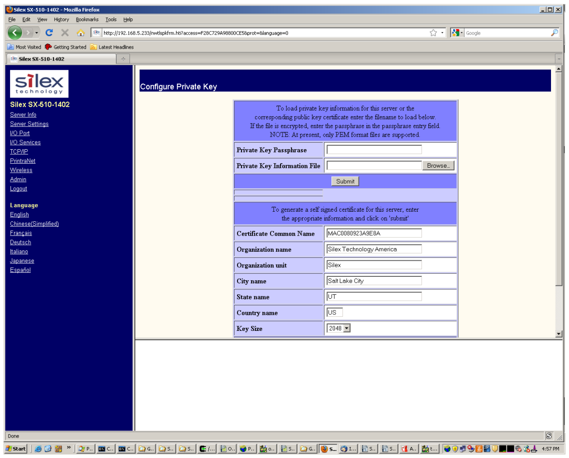
Certificate Root Key
Enter the authentication key used to verify the root certificate in the certificate chain provided by the authentication server. To set to null, send leave this field blank.

Certificate Root Key Exponent
This value must match the authentication server certificate value. The default is 65537 (x10001).

Certificate Common Name
Enter the name of the certificate on the primary authentication server. If both of the

6. Enter the filename containing the CA key certificate. used for the Authentication Server public key. Use the browse button if desired. Click submit to send the certificate to the SX-500.

To load SX-500 RSA public and private keys, return to the Network Security page and click on ***Configure Private Key.***



Configure Private Key

To load private key information for this server or the corresponding public key certificate enter the filename to load below. If the file is encrypted, enter the passphrase in the passphrase entry field. NOTE: At present, only PEM format files are supported.

Private Key Passphrase	
Private Key Information File	

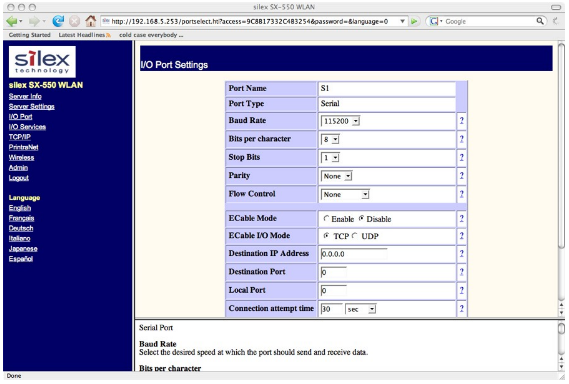
To generate a self signed certificate for this server, enter the appropriate information and click on 'submit'

Certificate Common Name	MAC0080923A9E8A
Organization name	Silex Technology America
Organization unit	Silex
City name	Salt Lake City
State name	UT
Country name	US
Key Size	2048

7. If you are entering an externally generated key pair, enter the file name, and PEM passphrase if required, in the upper form on the page. Click submit to send the key data to the SX-500. If the private key and public key certificate are in separate files, this will need to be done twice.

   If you wish to have the SX-500 generate the private key/public key self signed certificate pair for you, enter the desired information for the public key certificate in the second form on the page, and click on submit. When the generation operation is complete, the public key certificate may be retrieved by clicking on one of the links at the bottom of the page, in order to pass the certificate to the Authentication Server.

Now click ***I/O Port*** on the left side of the screen to configure the serial port.



I/O Port Settings

Port Name	S1
Port Type	Serial
Baud Rate	115200
Bits per character	8
Stop Bits	1
Parity	None
Flow Control	None
ECable Mode	○ Enable ● Disable
ECable I/O Mode	● TCP ○ UDP
Destination IP Address	0.0.0.0
Destination Port	0
Local Port	0
Connection attempt time	30 sec

Serial Port

Baud Rate
Select the desired speed at which the port should send and receive data.

Bits per character

8. Configure the serial port settings so that they match the settings on your device. For example, if your device is set for 9600bps, odd parity, and XON/XOFF flow control, you must change the settings on the Serial Device Server to these settings.

Click the ***Submit*** button at the bottom of the window (you may need to scroll) to save your changes.

When you have finished with all your configuration changes, you must restart the Serial Device Server for these changes to take effect.

You can skip the remainder of this chapter.

Using the Internal Command Console to Configure the Serial Device Server

You may skip this section if you have completely configured the SX-500 using the SX-500 Internal Web Pages.

The Internal Command Console is a command line oriented method for configuring the Serial Device Server. It provides more comprehensive capabilities than the Internal Web Pages, but is not as easy to use. Advanced users may prefer to use this method because it is concise, fast, and powerful.

To use the Internal Command Console:

1. To access the Internal Command Console, enter the following command from the Windows Command Prompt (MS-DOS Prompt), Mac OS X Terminal Utility, or UNIX/Linux command line:

   telnet *aa.bb.cc.dd*

   where aa.bb.cc.dd is the IP address of the Serial Device Server (for example, *telnet 192.168.5.6*).

2. Press <ENTER> and then enter the password (the default value is *access)* at the # prompt. Press <ENTER> at the *Enter Username*> prompt. When you see the *Local*> prompt, you can enter console commands.

3. If you used the default 192.0.0.192 IP address to connect to the Serial Device Server, you MUST change it to a new valid IP address. If necessary, you must also change the Subnet Mask and Router (Gateway). The commands are as follows:

   SET IP ADDRESS *aa.bb.cc.dd*

   SET IP SUBNET *aa.bb.cc.dd*

   SET IP ROUTER *aa.bb.cc.dd*

   where *aa.bb.cc.dd* is the IP address of the Serial Device Server. You can use the command SHOW IP to verify the IP address settings.

4. Enter the basic wireless settings as follows:

SET NW SSID <name>	*[where <name> is the SSID for your network]*
SET NW MODE <mode>	*[where mode is INFRASTRUCTURE or AD-HOC]*
SET NW CHANNEL n	*[where n is 1 to 11; this is only used in AD-HOC MODE]*

5. Use the appropriate SET NW command to set wireless encryption mode and authentication type (check with your network administrator for the proper settings if you do not know them):

   SET NW ENC <mode> *[sets encryption mode, where <mode> is WPA, WPA2, 64, 128, or WPA2-WPA]*

   SET NW AUTHTYPE <type>   *[sets authentication type, where <type> is OPEN, SHARED, TTLS, PEAP, WPA-PSK, LEAP, or TLS].*

For WPA2-PSK or WPA-PSK, enter the command:

```
SET NW WPAPSK <psk>         [sets pre-shared key for WPA2 or WPA, where <psk> is
                                     the key]

SET NW WPAGROUP <state>  [enables or disables WPA group key mode, where
                                     <state> is ENABLED or DISABLED; default is
                                     DISABLED]
```

For WEP (WEP64 or WEP128), use the following commands:

```
SET NW KEYVAL <key>         [Sets WEP key, where <key> is 10 hex characters for
                                     WEP64 or 26 hex characters for WEP128]
SET NW KEY#  n         [sets the number of the WEP key that will be used as the
                                     transmit key, where n=1 to 4; default value is 1]
```

Configuring 802.1X EAP authentication can be complex. Please refer to Appendix A and/or Appendix B for details of the required commands.

6. To set the serial port, enter the following commands:

```
SET PORT S1 SPEED <baudrate>       [where <baudrate> is 300 to 921600]
SET PORT S1 PARITY <parity>        [where <parity> is ODD, EVEN, MARK, or
                                    SPACE]
SET PORT S1 SIZE <databits>        [where <databits> is 7 or 8]
SET PORT S1 FLOW <flowcontrol>     [where <flowcontrol> is NONE, XON/XOFF,
                                    CTS, or DSR]
```

The console commands are summarized in Appendix B of this manual.

7. When you have finished entering commands type:

```
INIT
EXIT
```

These commands will save the configuration and restart the unit. You are now ready to use the Serial Device Server.

IMPORTANT: The console command EXIT must always be used in order to save the changes you made with the internal command Console.

8. Note that you can also access the Internal Command Console in the following ways:

   - *Internal Web Pages.* Use a web browser to connect to the Serial Device Server internal web pages as described earlier in this chapter. After you have logged in, click ***Admin*** on the left side of the screen, and then click ***Console***. You can now enter console commands (you must click ***Enter*** after each command).

Chapter 4
Using the Serial Device Server with Your Application

The Serial Device Server includes a number of capabilities that enable it to be used in a wide range of applications. These capabilities include:

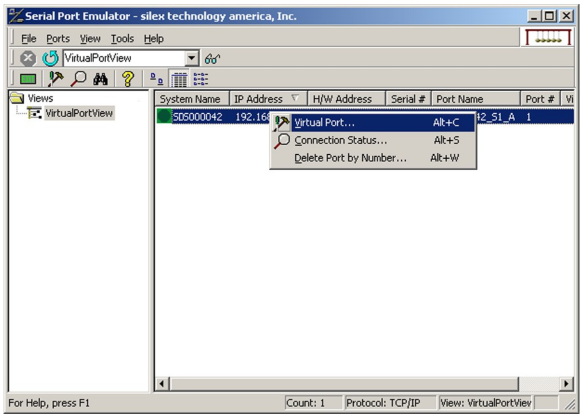
1. Serial Port Emulator (SPE) software
2. Raw TCP connection
3. RFC2217
4. ECable Mode
5. Print Server mode
6. FTP
7. Console mode switching
8. AT commands

These methods are described in the following sections.

Serial Port Emulator

The Serial Port Emulator (SPE) software emulates a standard Windows COM port. That is, it creates a virtual COM port that functions exactly like the Windows COM1 and COM2 serial ports, except that the I/O actually goes out over the Ethernet or WLAN to the Serial Device Server and to the serial device that is connected to the Serial Device Server. As a result, any application program that uses a standard Windows COM port can also use the Serial Port Emulator. The SPE is therefore especially useful if you have existing programs that use Windows COM ports.

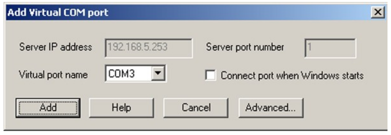
The SPE software is a component on the CD-ROM that is included with the Serial Device Server, or it can be downloaded from the Silex website. To install it, double click on the installer icon and follow the installation instructions. When the installation is complete, you can run the SPE software by clicking ***Start -> Programs -> Silex technology -> Serial Port Emulator -> Serial Port Emulator.***


Serial Port Emulator - silex technology america, Inc.
File Ports View Tools Help
VirtualPortView
Views
VirtualPortView
Virtual Port... Alt+C
Connection Status... Alt+S
Delete Port by Number... Alt+W

System Name	IP Address	H/W Address	Serial #	Port Name	Port #	Vi
SDS000042	192.168			42_S1_A	1	

For Help, press F1 | Count: 1 | Protocol: TCP/IP | View: VirtualPortView

After the Serial Port Emulator software has started, you will see a list of all the configured Serial Device Servers on the network. Right click on the name of the Serial Device Server that you want the virtual COM port to connect to (the default name is SLX*xxxxxx*, where *xxxxxx* is the last six digits of the Serial Device Server MAC address), and then click ***Virtual Port***. You will be asked to select the name of the virtual COM port (for example, COM3).



Server IP address: 192.168.5.253

Server port number: 1

Virtual port name: COM3

□ Connect port when Windows starts

Click ***OK*** after you have selected the name, and you now ready to use the virtual COM port.

Using virtual COM port is identical to using a normal COM port. For example, if you configure a virtual COM port called COM3, this port will show up as one of the available serial ports when you use the Windows HyperTerminal Accessory program.

Raw TCP connection

You can communicate directly from your application program to the Serial Device Server using a raw TCP connection. This is done by opening a TCP port on the Serial Device Server and then sending and receiving data to this port via a socket or equivalent API. This method is more efficient than using the Serial Port Emulator, and does not require any additional software to be installed on your computer.

If you are using a raw TCP connection, the default TCP port number (you can use any or all of these port numbers) for normal connections. If you want to be able to access your device's modem control signals from your computer system, then the TCP port number is 9200 (this enables RFC 2217 support). You can change the port number, if desired, by modifying one of the Serial Device Server services. To change the TCP port number:

1. Connect to the Serial Device Server with a web browser (see chapter 3 for instructions on doing this);
2. After you have logged in, click ***I/O Services*** on the left side of the page.
3. Click on the service name that you want to change (any one of the services is OK, provided that you are not using the existing TCP port number of that service for a different application).
4. Change the ***Raw TCP Port*** to the desired number (must be greater than 1023).
5. Click ***Submit*** to save your change.

You can test this connection by using the TELNET utility from the Windows Command Prompt (MS-DOS prompt), Mac OS X Terminal Utility, or UNIX/Linux command line as follows:

```
telnet ipaddress portnumber
```

where i*paddress* is the IP address of the Serial Device Server and *portnumber* is the Serial Device Server TCP port number. For example:

```
telnet 192.168.5.53 9100
```

In this example, if you have a serial printer or other device capable of displaying ASCII characters connected to the Serial Device Server serial port, then every character you type should be printed on that serial device (buffered serial devices may need you to type a control character such as a formfeed (CONTROL-L) before the characters are printed).

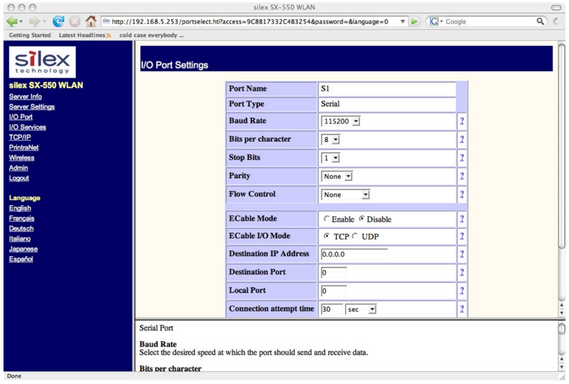
RFC 2217 Remote Modem Control Support

RFC 2217 allows you to access your device's modem control signals over the network. It is especially useful for migrating applications that use modem controls from a direct serial connection to a serial device server network connection. You can utilize RFC 2217 from the Silex Serial Port Emulator software (see below), or by connecting to TCP port 9200 from your application program.

ECable Mode

Normally, it is up the computer to initiate a connection to the Serial Device Server. For some applications, it is desirable for the Serial Device Server to initiate the connection to the computer. The Serial Device Server supports this capability through its ECable feature.

To set ECable mode, use a web browser to access the Serial Device Server internal web pages (see chapter 3 for instructions on using the internal web pages). After you have logged in, click I/O port on the left side of the screen.



I/O Port Settings

Port Name	S1
Port Type	Serial
Baud Rate	115200
Bits per character	8
Stop Bits	1
Parity	None
Flow Control	None
ECable Mode	○ Enable ● Disable
ECable I/O Mode	● TCP ○ UDP
Destination IP Address	0.0.0.0
Destination Port	0
Local Port	0
Connection attempt time	30 sec

Serial Port

Baud Rate
Select the desired speed at which the port should send and receive data.

Bits per character

You can now enable ECable mode and set the required parameters.

1. Enable ECable mode by clicking the radio button.
2. Enter the address (Destination Address) of the computer or other device that will be communicating with the Serial Device Server)
3. Enter the TCP port number (Destination Port) used by the destination device for communicating with the Serial Device Server (must be greater 1023).
4. If desired, change the ECable Connection Attempt Time. This specifies the time interval between connection attempts. For example, by default the Serial Device Server will try once every 30 seconds to make a connection to the destination device; if it fails to make this connection, it will wait 30 seconds before attempting again. Changing this interval will reduce or increase the amount of network traffic.
5. It is also possible to use UDP instead of TCP for communicating to and from the Serial Device Server. If you wish to use UDP, then:

a. Select UDP as ECable I/O Mode.
b. Enter the UDP port number (Destination Port) used by the destination device to communicate with the Serial Device Server. This number must be a valid port on the destination device (check the documentation for that device to determine the valid port numbers).
c. Enter the UDP port number (Local Port) used by the Serial Device Server to communicate with the destination device. This number must be greater than 1023, but is otherwise arbitrary.

NOTE: ECable mode cannot be used in conjunction with the Serial Port Emulator software.

Print Server Mode

You can use the Serial Device Server as a standard TCP/IP print server, which is very useful if you are connecting the Serial Device Server to a serial printer. The Serial Device Server supports the following standards:

- *lpr/lpd*. This is one of the most popular ways to print on a TCP/IP network. Check your computer's documentation to determine how to set up an lpr print queue. Usually this simply involves specifying the IP address of the Serial Device Server as the printer's address or host name. Some implementations require a queue name; this name is the name of any of the Serial Device Server services. To see the names of the Serial Device Server services, connect to the Serial Device Server with a web browser (see chapter 3 for instructions on doing this); after you have logged in, click I/O Services on the left side of the page.

- *Port 9100*. This method is used to set up a Windows Standard TCP/IP port or for compatibility with software that supports the HP JetDirect Print Server (for example, HP Web JetAdmin). To use this capability on Windows with the *Add Printer Wizard*, specify that you want to use a ***Local printer attached to this computer*** (not a network printer), and then select ***Create a new port***, specifying ***Standard TCP/IP Por***t as the type of port.

  It is also possible to change the TCP port number from the default 9100 for compatibility with other printer manufacturer's software. To do this, refer to the instructions in the *Raw TCP Connection* section of this chapter.

FTP

The Serial Device Server supports FTP binary or ASCII communications. This can be used, for example, to send the contents of a file from a PC to a device connected to the Serial Device Server using the FTP protocol. To use FTP, simply enter the standard FTP command from your PC with the IP address of the Serial Device Server (for example, ftp 192.168.5.50). When the connection is made, enter any username and password. You can then use the standard FTP *put* command to send the file from the PC to the device connected to the serial port on the Serial Device Server.

Console Mode Switching

The Serial Device Server allows you to dynamically switch the operation of the serial port from normal mode to console mode. This allows your device to control the operation of the Serial Device Server by sending console commands (see chapter 6 and Appendix B for a description of the console commands). Note that console mode can only be entered when there is no connection to a remote host.

NOTE: The serial port console mode cannot be used in a FIPS 140-2 approved mode. The Cryptographic Officer must leave the console string as NULL (the factory default value).

To switch the serial port to console mode, you must first define a console string. When the Serial Device Server receives this string on the serial port, it will automatically switch the port to console mode. To define the console string, use a web browser to access the Serial Device Server internal web pages. After you log in, ***click I/O Port,*** and then select the desired port (S1 for the serial port). When you get the ***I/O Port Settings*** page, enter any desired character string (for example, xyz) as the ***Console Mode String***. Click ***Submit*** to save your string, and then restart the Serial Device Server to make the change take effect.

Alternatively, you can define the console mode string using the console command from TELNET as shown in the following example:

```
SET PORT S1 CONSTR xyz
```

Once you are connected in console mode, you can send any of the console commands listed in Chapter 5. Be sure to terminate each console command with a carriage return (ASCII 13) or linefeed (ASCII 10) character.

When you are finished using the console, you can return to the normal port operation by sending the command EXIT followed by a return or linefeed character.

AT Commands

The Serial Device Server allows you to control the serial port using standard AT modem commands. This allows you, for instance, to initiate connections and to switch between console mode and data mode by sending the appropriate commands. These capabilities are similar to the console mode switching described in the previous section, but have the following advantages:

- Your device can initiate a network connection
- Operation is compatible with software that uses the AT command set

The drawback, however, is that there is a slight delay when switching from data mode to AT command mode.

NOTE: The AT Command filter cannot be used in a FIPS 140-2 approved mode. The Cryptographic Officer must leave the port filter setting as TRAP (the factory default value).

To use the AT commands, you must first enable this capability using the ***I/O Port Settings*** internal web page for the serial port (S1). Change the ***Port Filter*** setting to AT in order to enable AT mode on that port and press the ***Submit*** button to save the change. You must restart the Serial Device Server to make the change take effect.

You can also use the console to enable the AT capabilities. For example, the command

```
SET PORT S1 FILTER AT
```

enables AT capabilities on the serial port.

Note: If you use the AT commands on the serial port, you cannot use SNMP traps or Email alerts or Console Mode for that port.

The AT commands are described in detail in Chapter 5.

Chapter 5
Advanced Configuration

The Serial Device Server Serial Device Server is equipped with a default configuration that works with most serial-to-Ethernet connections. You can modify the settings to suit your installation requirements.

The web browser interface is the recommended method for setting advanced configuration parameters. However, regardless of the method to access the configuration parameters, the method for modifying the parameters is virtually identical.

Factory Default Settings

Table 3 displays the serial port configuration parameter descriptions and settings with the default settings indicated in a separate column.

Table 3 Factory Default Settings

Parameter	Description	Settings	Default Setting
Character	Bits per character	7, 8	8
Flow	Flow control	None, XON, XOFF, CTS/RTS	None
Parity	Parity	None, Even, Odd, Mark, Space	None
Speed	Baud rate of bits per second	300, 600,1200, 2400, 3600, 4800, 7200, 9600, 14400,19200, 38400, 57600, 76800, 115200, 230400, 460800, 921600	115200
Stop	Stop bits per character	1, 2	1
Ecaddr	ECable destination IP address	Set by user	N/A
Econn	ECable connection attempt time	1-255 seconds	30 seconds
Ecport	ECable destination TCP port number	Set by user	N/A
Eclport	ECable destination local IP port	Set by user	N/A

Parameter	Description	Settings	Default Setting
	number (required for E-Cable UDP mode only)		
Ectmmsec	Cable connection time resolution	Enable, Disable	Disable
Ecudp	ECable UDP mode	Enable, Disable	Disable

Restoring Factory Default Settings

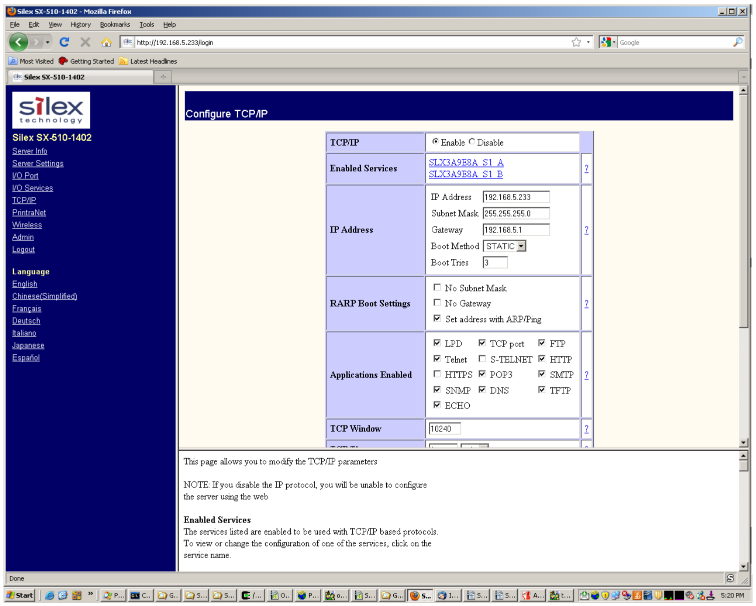
The factory default settings can be restored at any time To do this, hold down the Reset pushbutton for more than five seconds.

Modifying TCP/IP Settings

You can modify the TCP/IP settings using the web browser interface or the Serial Device Server Serial Device Server's internal configuration console.

To modify TCP/IP settings:

1. You can configure the TCP/IP settings using the Web Page configuration. Simply log in using the Serial Device Server IP address and select ***TCP/IP***.



Configure TCP/IP

TCP/IP	● Enable ○ Disable
Enabled Services	SLX3A9E8A_S1_A SLX3A9E8A_S1_B
IP Address	IP Address 192.168.5.233 Subnet Mask 255.255.255.0 Gateway 192.168.5.1 Boot Method STATIC Boot Tries 3
RARP Boot Settings	□ No Subnet Mask □ No Gateway ☑ Set address with ARP/Ping
Applications Enabled	☑ LPD ☑ TCP port ☑ FTP ☑ Telnet □ S-TELNET ☑ HTTP □ HTTPS ☑ POP3 ☑ SMTP ☑ SNMP ☑ DNS ☑ TFTP ☑ ECHO
TCP Window	10240

This page allows you to modify the TCP/IP parameters

NOTE: If you disable the IP protocol, you will be unable to configure the server using the web

Enabled Services
The services listed are enabled to be used with TCP/IP based protocols. To view or change the configuration of one of the services, click on the service name.

Figure 2 TCP/IP Window

2. Verify the settings, as defined in Table 4.

Table 4 TCP/IP Settings

Parameter	Setting
IP Address	To assign a static IP address, enter it in this field The IP address must follow the format XXX.XXX.XXX.XXX, where each XXX is a number between 0 and 255. The default IP address mask is 192.0.0.192.
Subnet Mask	To assign a static subnet mask, enter it in this field The subnet mask must follow the format XXX.XXX.XXX.XXX, where each XXX is a number between 0 and 255. The default subnet mask is 0.0.0.0. The server interprets a subnet mask of 0.0.0.0 or 255.255.255.255 as no subnet mask specified.
Default Gateway	Sets the default gateway, if your network is attached to other networks
Boot Method	Set to STATIC for a static IP address, set to DHCP or AUTO to attempt to automatically assign the IP parameters from a network server.
TCP Timeout	Sets the timeout and reset values for the TCP connections
Keepalive Timer	Blocks or broadcasts unsolicited ARP used to notify access point or router that the unit is still connected.
DNS	Sets the DNS addresses

3. For the changes to become effective, click the ***Submi***t button, then reset the Serial Device Server.

Using AT Modem Commands

NOTE: The AT Command filter cannot be used in a FIPS 140-2 approved mode. The Cryptographic Officer must leave the port filter setting as TRAP (the factory default value).

The Serial Device Server firmware has an optional data filter for configuring using AT style modem commands with the serial port. This feature allows devices with an existing AT command interface to configure the unit, if the AT commands can be properly modified. You must be familiar with the general operation of AT commands. Note that AT command processing is not enabled by default. Use the command SET PORT S1 FILTER AT to enable this feature.

All commands begin with AT and are terminated by a new line unless noted below. While standard AT commands are defined to be 40 characters or less (not including the AT), the server accepts commands of up to 80 characters.

Standard AT Commands Supported

The Serial Device Server recognizes a subset of the standard AT command set. The data channel must be in the command mode for commands to be recognized. The data channel will be in command mode upon power up or reset.

There are two operating modes for the unit when the AT command option is enabled. In command mode, data received from the serial port is passed to the AT command processor, and responses are returned to the serial port. No data is sent to any network application, and any data received from the network is ignored. In data mode, data from the serial port passes to the network application, and vice versa. This is equivalent to the normal serial port operating mode without the AT command option.

Table 5 describes the AT Commands. Table 6 details the Extended AT Commands that allow the configuration of the network server operating parameters. Any AT command received, except the listed commands, are acknowledged with OK status. This allows existing modem applications to transmit commands without causing an error. These include AT<X>n, but not currently AT&<X>n, AT%<X>n, AT\<X>n, where <X> is a letter.

Table 5 AT Commands

Parameter	Command	Description
Enter Command mode	<delay>+++<delay>	If the string +++ is seen in data mode, with no characters sent for 1 second before or after, then command mode is entered.
Initiate Connection Command	ATD <destination>	Standard modem dialing command, redefined to initiate an internet connection to a remote computer. Indicates the IP address of the target, and optionally the TCP port number to use for connection. The T or P option (ATDT or ATDP) can be present and has no effect. If present, the IP address must be exactly 12 decimal digits with 3 for each byte of the address. If no IP address is given, then the ECable destination address defined for the port is used. If the destination TCP port is defined, it is separated from the IP address by a '#' character, and is 1 to 5 decimal digits. If TCP port is defined, the ECable destination port defined for the serial port is used. If the destination port is 0, the standard Telnet port (23) is used. If the destination string ends with a semicolon, the server remains in the command mode, not the data mode, once a connection is made. In command mode data is not passed from the remote computer, so data could be lost if the unit stays in command mode. If the connection cannot be attempted, NO CARRIER status is returned. If the connection attempt fails, NO ANSWER status is returned. If the connection succeeds, CONNECT status is returned.

Parameter	Command	Description
Echo control	ATEn	If n=0, commands are not echoed. If n=1, subsequent commands will be echoed. The default, upon unit reset, is for no echo (ATE0).
Disconnect	ATHn	If n=0, any connection to a remote host is dropped. Other value of n is ignored.
Return to data mode	ATOn	Exits command mode and places the serial port in the data mode. All subsequent data is sent to the network application, if connected, until an enter command mode sequence is received. Any value of n is ignored, if present.
Quiet mode	ATQn	If n = 1, no result codes are returned. If n = 0, result codes are returned to the local device. 0 is the reset default value.
Verbose mode	ATVn	If n = 0 and not in quiet mode, result codes are returned in numerical form. If n = 1, results are returned as text. 1 is the reset default value.

Table 6 Extended AT Commands

Parameter	Command	Description
Console pass through	AT#C<string>	Passes the string to the server configuration console. The string can be any valid console command. Refer to your server documentation for console commands available on your unit. Since this command does not follow the normal AT command format of <command><number>, it must be the last command on the line unless the next command is a '#' command. All characters up to the end of line or a '# will be considered part of the console command. If console quiet mode is not is enabled, then the response will be the standard console task response. Example: `AT#Cset nw ssid silex#Csave`
Console Quiet mode	AT#Qn	If n = 0, a response to a #C command is given. If n = 1, the response is not provided. The default after reset is 1.

Response Codes

Table 7 details the response codes for codes other than #C commands.

Table 7 Response Codes

Numeric Code	Description
0	OK
2	No Carrier
4	Error
5	Connect
8	No Answer

Chapter 6
Troubleshooting

If you have experience problems with the Serial Device Server, please check the following troubleshooting steps:

1. Make sure that you are getting power to the Serial Device Server. The orange LED should be on solid if the proper power is being received. If it is not on, check the power supply connections, and if possible, try a different Silex Serial Device Server power supply.

2. Make sure that you have a valid network connection.

    a. Make sure that your network is operating properly (that is, other devices should be able to communicate using the same hub, switch, or access point that the Serial Device Server is connected to).

    b. If you are using hardwired Ethernet, the green LED should be lit or blinking. If it is not, make sure that the cable is properly connected, and if possible, try a different Ethernet cable.

    c. If you are using a wireless connection, both the yellow LED and green LED should be lit or blinking. If they are not, double check your wireless settings. The SSID and security parameters must exactly match the requirements of the access point in order for the Serial Device Server to communicate on an infrastructure wireless network. If you are using Ad-Hoc mode, the Serial Device Server must have exactly the same SSID, security parameters, and RF channel as the other wireless device(s) on the network.

    d. Make sure that you have a valid IP address, subnet mask and router address (check with your network administrator to make sure that you have the correct information). You can check to see if the IP address information is correctly set by printing a test page (press the RESET pushbutton to send a test page to a printer or terminal connected to the serial port) or by using the PING command from a computer system connected to the network.

3. If you have a valid network connection and IP address, but you cannot communicate with your serial device, then:

    a. Make sure that the settings of the serial port on your device exactly match the settings of the serial port of the Serial Device Server. For example, if your device is set for 9600bps, 8-bit characters, no parity, and RTS/CTS flow control, the Serial Device Server must also have these exact same settings.

b. Make sure that have a good cable connection between your serial device and the Serial Device Server. If possible, try a different cable.

c. Make sure that the cable pinouts are correct. In order to communicate properly, the transmit data line on the Serial Device Server must be connected to the receive data line on your serial device, and the receive data line on the Serial Device Server must be connected to the transmit data line on your serial device. Modem signals, if any, must also be connected so that input signals are connected to output signals and vice-versa. Refer to the cable diagrams in Chapter 2 of this manual.

d. Try printing a test page (if your serial device is not capable of directly displaying ASCII character output from the Serial Device Server's serial port, then disconnect the device and connect a serial printer or terminal to the Serial Device Server). If the test page prints OK, then the serial port on the Serial Device Server is working properly. If it does not print, then double check steps 3a, 3b, and 3c.

If none of the above steps solves your problem, then check the Support and Downloads section of the Silex website (www.silexamerica.com). You can also contact Silex support by phone, Email, or fax as follows:

Hours of Operation: Monday-Friday 8:00am-5:00pm MST
Phone: **US toll free:** (866) 765-8761, **International:** 1 (801) 748 - 1199, **Fax:** 1 (801) 748-0730
Email: Tech support: support@silexamerica.com,

Be sure to have the following information ready when you call Silex support:

1. Model number and serial number of the Serial Device Server
2. Firmware version of the Serial Device Server
3. Your hardware and software environment:
    a. Your CPU and operating system
    b. Type of device that you are connecting to the Serial Device Server
    c. Wireless/wired networking environment (for example, access point manufacturer/model, wireless security, routers, etc.)
4. Description of the problem

Chapter 7
Product Specifications

Table 8 Product Specifications

Component	Specifications
Model	SX-500 Serial Device Server
Processor	Cavium NITROX Soho CN210
RAM Memory	16 Mbytes SDRAM.
Processor Speed	167 MHz

Interfaces Supported	Serial: RS-232-C;
	Ethernet: 10/100BaseT
	Wireless: 802.11b/g (SX-500);

Dimensions	SX-500: 125.73 x 75.11 x 24.08 mm (4.95 x 2.957 x 0.948 inches), not including mounting brackets or connectors
Temperature	0 to 50 degrees C (operating); -20 to 70 degrees C (storage); maximum 20 degrees C change per hour
Humidity	10% to 90% non-condensing
Altitude	3.1km (operating); 9km (storage)
Electrical	Wired models: 500mA@+5VDC Wireless models: 800mA@+5VDC Power provide through external AC adapter (included) or via pin 9 on the 9-pin serial port connector

Table 9 Radio Performance Specifications

Parameter	Specifications
Radio Emission Type	Complies with IEEE 802.11 b, g, h and j Direct Sequence Spread Spectrum (DSSS) physical layer.
Operating Frequency	2.412 GHz ~ 2.484 GHz ISM band
Data Modulation Type	Orthogonal Frequency Division Multiplexing (OFDM) Complementary Code Keying (CCK)

Parameter	Specifications
	Differential Quadrature Phase Shift Keying (DQPSK) Differential Binary Phase Shift Keying (DBPSK)
Channel Number	IEEE 802.11b and g: Channels 1 to 11 and 12 to 14
Data Rate	54 Mbps with fallback rates of 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, and 1 Mbps
Security	Encryption: WEP 64/128 bits, WPA (TKIP), WPA2 (AES) Authentication: WEP Open System and Shared Key; WPA-PSK, WPA2-PSK, 802.1X with LEAP, TLS, TTLS, and PEAP
Media Access Protocol	Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with ACK architecture, 32 bits MAC-layer.
Antenna Connector Type	2 SMT ultra-miniature coaxial connectors
Operating Voltage	5 VDC ± 5%, 600mA (wireless), 500mA (wired)
Bus Interface	Proprietary 70-Pin
Antenna Port Impedance	50 ohm

TCP Port Connections

The Serial Device Server supports port connections over TCP/IP for data transfer to the serial port using raw TCP ports only. Table 10 describes the TCP ports allocations.

Table 10 TCP Port Connections

Port	Destination Device
3001	RS-232
9100	RS-232
9200	RFC 2217

Appendix A
Advanced Security Configuration

There are numerous possible security settings. It is therefore important that you verify the appropriate settings with your network administrator. If you enter the settings incorrectly, the Serial Device Server will not be able to communicate on your network. The following table summarizes the wireless settings required for each encryption mode and authentication type. The bold values are those which are FIPS 140-2 approved.

		Authentication Type							
		Open System	Shared-Key	PSK	802.1x				
					TTLS	LEAP	PEAP	TLS	EAP-FAST
Encryption Mode	Disable	(OK)	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	64-Bit WEP	1	1	N/A	N/A	N/A	N/A	N/A	N/A
	128-Bit WEP	1	1	N/A	N/A	N/A	N/A	N/A	N/A
	WPA	N/A	N/A	2, 3	4, 7	4	4, 5, 6	4, 5, 6	N/A
	WPA2	N/A	N/A	**2, 3**	4, 7	4	**4, 5,6**	**4, 5, 6**	N/A
	WPA2-WPA	N/A	N/A	2, 3	4, 7	4	4, 5,6	4, 5, 6	N/A
	Dynamic WEP	N/A	N/A	N/A	4, 7	4	4, 5,6	4, 5, 6	N/A
	Wired Ethernet Network	N/A	N/A	N/A	4, 7	N/A	4, 5,6	N/A	N/A

Basic Configuration Parameters
1. 64/128Bit WEP Key
2. WPA-PSK
3. WPA Group Key

802.1X Configuration Parameters
4. User ID and Password
5. Authentication Server Certificate
6. Private Key/Public Key Certifcate
7. Authentication Protocol

To use the above table, select the encryption mode and authentication type you are using. For example, if you are using WPA2 with PSK authentication, you would need to set the WPA-PSK pre-shared key and enable or disable the WPA Group Key. Likewise, if you are using WPA2 with 802.1X TLS authentication, you would need to enter a User ID and Password, an Authentication Certificate, and a Private Key with corresponding public key certificate..

The following is a description of the authentication settings used by the Serial Device Server:

Encryption Mode (Wireless Security Only)
The possible Serial Device Server wireless encryption modes include:

- *64 and 128 bit WEP.* These are available for basic WIFI compatibility. Because of known security issues, WEP should be avoided if possible.
- *Dynamic WEP*. Dynamic WEP uses WEP encryption with an 802.1X EAP authentication method. It is not necessary to set keys with this method, because they are automatically assigned.
- *WPA2*. WPA2 is the latest and strongest wireless security standard. It uses CCMP encryption. Like WPA, it can be used either with a pre-shared key or with 802.1X authentication.
- *Wi-Fi Protected Access (WPA*). WPA uses TKIP encryption, and can be used with either a pre-shared key (PSK) or with 802.1X authentication.
- *WPA2-WPA*. This mode combines the capabilities of WPA2 and WPA by using CCMP for pairwise encryption, but allowing TKIP for group encryption.

NOTE: FIPS 140-2 approved operation requires WPA2 (AES-CCMP) encryption

To set the encryption mode, select the desired mode from the pull down menu on the Configure Network Security screen in the Serial Device Server internal web pages, or use the console command SET NW ENC <mode>, where <mode> is DISABLE, 64, 128, WPA, OR WPA2.

Note that the encryption mode only applies to wireless networks, so it is not necessary to set this mode if you are using a wired Ethernet network.

Key Selection (Wireless Security Only)
This parameter selects which of the four possible WEP keys will be used as the transmit key (the first key is the default). Select the desired key selection from the pull down menu on the Configure Network Security screen in the Serial Device Server internal web pages, or use the console command SET NW KEY# *n*, where n is 1, 2, 3, or 4.

WEP Key Value (Wireless Security Only)
Up to four keys can be entered if you are using WEP security. The value of the keys must be entered as hexadecimal digits (up to 10 hex digits for 64 bit WEP or 26 hex digits for 128 bit WEP). Enter the desired key value(s) on the Configure Network Security screen in the Serial Device Server internal web pages, or use the console command SET NW KEYVAL <key>, where <key> is 10 hex digits for WEP64 or 26 hex digits for WEP128.

Pre-Shared Key (Wireless Security Only)
If you are using WPA2 or WPA with the PSK mode of authentication, the key value entered here is used to initialize the session with the access point. If a key value is entered, it must be exactly 64 hex characters. Enter the desired PSK on the Configure Network Security screen in the Serial Device Server internal web pages, or use the console command SET NW WPAPSK <psk>, where <psk> is the key.

WPA Group Key (Wireless Security Only)
If the WPA Group Key mode is enabled, then group keys may be used for data link encryption (the default is disabled). Select whether to enable or disable the WPA Group Key on the Configure Network Security screen in the Serial Device Server internal web pages, or use the console command SET NW WPAGROUP <state>, where <state> is ENABLED or DISABLED.

NOTE: For FIPS 140-2 approved operation, this parameter must be DISABLED.

Wireless Authentication Type (Wireless Security Only)

This parameter sets the type of authentication to be performed with the network access point (Radius authentication server), or with a peer unit in Ad Hoc mode. The Serial Device Server supports Shared Key and Open System Authentication with WEP, and PSK, TLS, TTLS, LEAP and PEAP with WPA, WPA2, DYNAMIC WEP, and WPA2-WPA. Select the desired wireless authentication type on the Configure Network Security screen in the Serial Device Server internal web pages, or use the console command SET NW AUTHTYPE <type>, where <type> is OPEN, SHARED, TTLS, PEAP, WPA-PSK, LEAP, or TLS,.

NOTE: For FIPS 140-2 approved operation, this parameter must be TLS, PEAP or PSK

Wired Authentication Type (Wired Ethernet Networks Only)

This parameter sets the type of authentication to be performed with a Radius authentication server on a wired Ethernet network. The Serial Device Server supports TLS, TTLS, and PEAP authentication on these types of networks. Select the desired wired authentication type on the Configure Network Security screen in the Serial Device Server internal web pages, or use the console command SET NW ETHAUTH <type>, where <type> is TTLS, TLS or PEAP.

Authentication Attempts

This parameter sets the number of authentication attempts to make before the Serial Device Server assumes the network has no authentication. If zero (0) is entered, the Serial Device Server attempts to authenticate forever. Enter the number of authentication attempts on the Configure Network Security screen in the Serial Device Server internal web pages, or use the console command SET NW AUTHTRY *n*, where *n* is the number of attempts (default is 0).

User ID

This parameter is the logon user ID that the Serial Device Server uses to authenticate to the 802.1x-enabled network. The user ID and password must be in the authentication server database. The default user ID is 'anonymous'. Enter the user ID on the Configure Network Security screen in the Serial Device Server internal web pages, or use the console command SET NW ID <user id>, where <user id> is the user ID (the realm can included in the user id with the separator “@”).

Realm

A realm defines a grouping of users. If a realm is required for your network, it is separated from the user ID by a '@' character. Among other things, realms make it easier to segregate user groups into independently administered databases, to apply policies on a user group basis, and to establish roaming agreements. The default realm if not specified is 'anonymous'. Enter the realm on the Configure Network Security screen in the Serial Device Server internal web pages, or use the console command SET NW REALM <realm>, where <realm> is the name of the realm.

Password

This parameter is the logon password that the server uses to authenticate to the 802.1x-enabled network. The user ID and password must be in the authentication server database. The password may be a text string, or a string of hex bytes. Enter the password on the Configure Network Security screen in the Serial Device Server internal web pages, or use the console command SET NW PW <password>, where <password> is the password (default value is *anonymous*).

Authentication Protocol

This parameter determines how the server authenticates itself to the 802.1x-enabled network after an 802.1x session is established. The default is PAP; MSCHAP_V2 is the alternative protocol. Select the desired protocol on the Configure Network Security screen in the Serial Device Server internal web pages, or use the console command SET NW INAP <password>, where <password> is PAP or MSCHAP_V2.

Authentication Certificate

Authentication certificates are used by TLS and PEAP. You can manually enter the certificate information, or you can extract the Root Key and Root Key Exponent from a file on your disk. The required information is as follows:

- **Certificate Root Key** This is the authentication key used to verify the root certificate in the certificate chain provided by the authentication server. To set to null, send leave this field blank. Enter the certificate root key on the Configure Authentication Certificate page in the Serial Device Server internal web pages, or use the console command SET NW CERTKEY <value>, where <value> is the value of the key.

- **Certificate Root Key Exponent** This value must match the authentication server certificate value. The default is 65537 (x10001). Enter the certificate root key on the Configure Authentication Certificate page in the Serial Device Server internal web pages, or use the console command SET NW CERTEXP <value>, where <value> is the hexadecimal value of the key (default is 10001).

- **Certificate Common Name 1 and Certificate Common Name 2** This is the name of the certificate on the primary authentication server (most applications only use a single certificate common name). If both of the common names are set to null, all certificates are accepted. The default is null. Enter the names on the Configure Authentication Certificate page in the Serial Device Server internal web pages or use the console command SET NW CERTCN <name1> or SET NW CERTCN2 <name2> to enter the two certificate common names, where <name1> and <name2> are the desired names.

Private Key (TLS & PEAP Wireless Security Only)
Private key information or the corresponding public key certificate for the Serial Device Server can be loaded from a file (Private Key Information File). If the file is encoded, you must enter the passphrase in the passphrase entry field on the Configure Private Key page in the internal web pages of the Serial Device Server (NOTE: At present, only PEM format files are supported). To generate a self-signed certificate for the Serial Device Server, the following information is required:

- **Certificate Common Name**
- **Organization name**
- **Organization unit**
- **City name**
- **State name**
- **Country name**
- **Key Size (2048)**

You may enter this information on the Configure Private Key page in the internal web pages of the Serial Device Server, or via console commands.

Appendix B
Console Commands

The following tables describe the console commands available from the internal command console. Access the command console through the serial port (if enabled for console mode) or over the network using a Telnet session or a web browser. The console can also be accessed via UART level signals on connector CN5 on the Serial Device Server printed circuit board (this requires you to open the Serial Device Server enclosure and use a special cable and adapter board; it should only be used by qualified Silex personnel for diagnostic and troubleshooting purposes).

Wireless and Network Security Commands

The following group of commands configures network parameters.

Table 11 Network Commands

Command	Description

SH NW	Displays summary network information
	Sample output:
	`WiFi Mode = INFRASTRUCTURE`
	`WiFi SSID: silex`
	`Speed = 11`
	`Regulatory Domain = 704`
	`WiFi FW Ver = 1F 1.7.1`
	`AP density = LOW`
	`TTLS is Disabled`
	`WEP is Disabled`
	`Link DOWN`

SH NW SQ	Display wireless network signal quality
	Sample Output::
	`Signal Quality  = 93`
	`Signal Strength = 53`
	`Noise Level     = 135`

Command	Description
SET NW AUTHtype	Sets wireless authentication type The default value is Open System Format: `SET NW AUTHtype [OPEN | SHARED | TTLS | LEAP | PEAP | TLS | PSK ]` **NOTE: For FIPS 140-2 approved operation, this parameter must be TLS, PEAP or PSK**
SH NW AUTH	Shows wireless authentication type Sample output: `Authentication type= OPEN SYSTEM`
SET NW ETHAUTH	Sets Ethernet wired authentication type The default value is Open System Format: `SET NW ETHAUTH [TTLS | TLS | PEAP ]`
SH NW ETHAUTH	Shows Ethernet wired authentication type Sample output: `Authentication type= PEAP`
SET NW AUTHTRY	Sets number of times the Serial Device Server will attempt to authentication The default value is 0. Format: `SET NW AUTHTRY n`
SH NW AUTHTRY	Shows number of authentication tries. Sample output: `Authentication Try Count = 3`
SET NW CHannel	Sets WLAN ad-hoc channel number The valid numbers are 1 through 11. Format: `SET NW CHannel n`
SET NW ENC	Sets WLAN Encryption Mode. Supported modes are None, 64 bit WEP, 128 bit WEP, WPA, WPA2, WPA2-WPA The default value is Disable. Format: `SET NW ENC  [Disable | 64 | 128 | WPA | WPA2 ]` **NOTE: For FIPS 140-2 approved operation, this parameter must be WPA2.**
SH NW ENC	Shows the wireless encryption mode The deprecated command SH NW WEP also displays this information. Sample output:

Command	Description
	`WiFi encryption is Disabled`
SET NW KEY#	Selects the WLAN WEP key entry (the WEP key that will be used as the transmit key) The possible values are 1, 2, 3, or 4; the default value is 1. Format: `SET NW KEY#    n`
SET NW KEYVAL	Sets the WLAN WEP key entry to the specified hex value For WEP128, the key is 10 hex characters long; for WEP128, the key is 26 hex characters long; the default value is null. Format: `SET NW KEYVAL <key>`
SET NW MOde	Sets WLAN mode The possible modes are Infrastructure and Ad-Hoc; the default value is Ad-Hoc Format: `SET NW MOde   <mode>`
SH NW MODE	Shows wireless operating mode Sample output: `Wifi mode = AD-HOC (802.11)`
SH NW RADio	Shows the selected radio mode of operation Sample output: `Radio mode is 802.11b-g`
SET NW SPeed	Sets maximum WLAN speed Possible values are 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, and 1; the default value is 54. Format: `SET NW SPeed   n`
SH NW SPEED	Show the maximum wireless data speed in megabits per second Sample output: `Speed = 54`
SET NW SSid	Sets WLAN SSID The default value is *serserv*. Format: `SET NW SSid   <name>`
CL NW SSid	Clears SSID value and allows the server to connect to any AP. Format: `CL NW SSid`
SET NW BSsid	Sets WLAN BSSID to connect to a specific access point’s mac address Format: `SET NW BSsid  <value>`

Command	Description
CL NW BSsid	Clears BSSID value and allows the server to use SSID, not a specific AP Format: `CL NW BSsid`
SET NW RTS	Sets WLAN RTS threshold The possible values are between 1 and 3000; the default value is 2432. Format: `SET NW RTS     n`
SH NW RTS	Shows wireless RTS threshold Sample output: `Wifi RTS Threshold = 2432`

SH NW STATS	Shows network I/O statistics
	Sample output:
	`WiFi statistics:`
	`TX Unicast frames: 0`
	`TX Multicast frames: 0`
	`TX Fragments: 0`
	`TX Unicast octets: 0`
	`TX Multicast octets: 0`
	`TX Deferred: 0`
	`TX Single retry frames: 0`
	`TX Multiple retry frames: 0`
	`TX Retry limit exceeded: 0`
	`TX Discards: 0`
	`RX Unicast frames: 0`
	`RX Multicast frames: 0`
	`RX Fragments: 0`
	`RX Unicast octets: 0`
	`RX Multicast octets: 0`
	`RX FCS errors: 0`
	`RX Discards no buffer: 0`
	`TX Discards wrong SA: 0`
	`RX Discards WEP undecr: 0`
	`RX Msg in msg fragments: 0`
	`RX Msg in Bad msg fragments: 0`

SET NW CERTCN	Sets EAP Common Name The default value is null. Format: `SET NW CERTCN   <name>`

Command	Description
SH NW CERTCN	Shows the value of first common name check string The default is null (blank) string. The command SH NW TTCN also returns this information. Sample output: `Common name 1`
SET NW CERTCN2	Sets second EAP Common Name Format: `SET NW CERTCN2   <name>`
SH NW CERTCN2	Shows the value of the second common name check string The default is null (blank) string. Sample output: `Common name 2`
SET NW CERTEXP	Sets EAP Certificate Exponent value The default value is 10001 Hex. Format: `SET NW CERTEXP  <exponent>`
SH NW CERTEXP	Shows the value of the certificate exponent The deprecated command SH NW TTEXP also returns this value Sample output: `65537 (10001h)`
SET NW CERTKEY	Sets EAP root key Format: `SET NW CERTKEY  <key value>`
SET NW ID	Sets authentication User ID This can include the realm separated by @. The default value is anonymous. Sample output: `SET NW ID   <user id>`
SH NW ID	Shows the value of the authentication ID, including realm, if applicable The default realm is a null (blank) string. The deprecated command SH NW TTID also returns this data. Sample output: `anonymous@somewhere`
SET NW PW	Sets the password for the 802.1x EAP authentication, if enabled The default value is anonymous. Format: `SET NW PW   <password>`

Command	Description
SET NW INAP	Sets EAP inner-authentication protocol The possible protocols are PAP and MSCHAP_V2; the default value is PAP. Format: `SET NW INAP   [PAP|MSCHAP_V2]`
SH NW INAP	Shows the inner authentication mode The deprecated command SH NW TTAP also returns this data. Sample output: `Authentication protocol = PAP`
SET NW REALM	Sets the realm portion of the 802.1x EAP authentication ID This value can also be set with the ID command. The default value is null. Format: `SET NW REALM   <realm>`
SH NW REALM	Shows the realm associated with the authentication ID, if applicable. The default value is null (blank) string. The deprecated command SH NW TTRE also returns this data. Sample output: `Somewhere`
SET NW WPAGROUP	Enable or disable WPA group key mode. If enabled, group keys can be used for data link encryption. The default value is disabled. Sample output: `SET NW WPAGROUP [ENABLE | DISABLE]` **NOTE: For FIPS 140-2 approved operation, this parameter must be DISABLED.**
SH NW WPAAUTO	Shows state of WPA auto connect flag Sample output: `WPA-AUTO Enabled`
SH NW WPAGROUP	Shows state of the allow WPA group keys flag Sample output: `WPA-GROUP Disabled`.
SET NW WPAPSK	Sets WPA PSK pass phrase or hex key. This value is only used if the authentication mode is WPA-PSK or WPA2-PSK. The argument to this command is exactly 64 hex characters representing the 256 bit PSK value. Format: `SET NW WPAPSK <key>`

Command	Description
SET NW WPATRACE	Sets WPA trace level. This command is for internal diagnostic purposes only. The default value is 0 or disabled. Format: `SET NW WPATRACE nn` **NOTE: For FIPS 140-2 approved operation, this parameter must be 0**
SH NW DISCONN	Displays the current value of the network disconnection timer Sample output: `Disconnect Timer: 5`

SET NW DISCONN	Sets the period of the network link disconnection watchdog timer. In wireless infrastructure mode, this timer monitors the wireless link, and if the unit is not connected to an AP for the time specified, the unit is reset.
	`SET NW DISCONN nn`
	`N = 0       watchdog timer is disabled`
	`    1-255   watchdog timer period in minutes`
	The factory default value is 5 minutes.
	This timer also controls a receive activity monitor when the wireless network link is connected. If no packets are received during the time specified, and the link remains up, the unit will reset at the end of the time period.

SET NW RESET	This command stops, and then resets the wireless network interface. This will effectively disassociate the unit from an access point if it is connected. If the unit is in wireless infrastructure mode, the unit will then scan and attempt to reconnect to a suitable access point, if one is available. Format: `SET NW RESET`
ZEROKEYS	Zeroizes the module private key and WPA PSK key, as well as any temporary key values held in RAM. The unit will then automatically perform a soft reset. Note that if any wireless encryption is enabled, it will be impossible to connect to an access point until the necessary key information has been re-configured.

Port Commands

Table 12 Port Commands

Command	Description

SH PORT	Shows port parameters
	Sample output:
	`Port     Q-Size     Type       Attributes`
	`*S1         0      serial     115200 N 8 1 XON/XOFF`

CLEAR PORT S1 JOB	Aborts the active job on the port.

Command	Description
	If the remote host is connected, additional data received will be discarded. Format: `CL PORT S1 JOB`
SET PORT S1 FLOW	Sets serial port flow control to NONE, XON/XOFF, CTS, or DSR The default value is none. Format: `SET PORT S1 FLOW <flow>`
SET PORT S1 PARITY	Sets serial port parity to NONE, EVEN, ODD, MARK, or SPACE The default value is none. Format: `SET PORT S1 Parity <parity>`
SET PORT S1 SIZE	Sets data bits on the serial port The default value is 8. Format: `SET PORT S1 SIZE [7 | 8]`
SET PORT S1 SPEED	Sets serial port baud rate. Options for BAUD are 300, 600, 1200, 2400, 7200, 9600, 19200, 38400, 57600, 115200, 230400, 460800, 921600 The default value is 115200. Format: `SET PORT S1 SPEED <baudrate>`
SET PORT S1 STOP	Sets serial port stop bits per character The default value is 1. Format: `SET PORT S1 STOP [1 | 2]`
SET PORT S1 MODE	Sets serial port line mode The default value is 232. Format: SET PORT S1 STOP [232 | 422 | 485 | 485D]

Server Information Commands

Table 13 Server Information Commands

Command	Description
SET SERVEr Description	Sets server description string Format: `SET SERVEr  DEscription   <description-string>`
SET SERVEr NAme	Sets server node name The default value is TWC_xxxxxx, where xxxxxx are the last 6 hex digits of the MAC address.

Command	Description
	Format: `SET SERVEr  NAme   <name>`
SET SNMP CONtact	Sets system contact string The default value is null. Format: `SET SNMP CONtact  <string>`
SET SNMP LOCation	Sets system location string The default value is null. Format: `SET SNMP LOCation <string>`
SH SERIAL	Displays serial number of the unit Sample output: `Serial number is 9047595`

SH SERVEr	Shows server parameters
	Sample output:
	`Serial Server Serial # 9047595`
	`Address: 00-40-17-8A-0E-2B     Name: TWC_8A0E2B Number: 0`
	`Identification:  Network Server`
	`Enabled Characteristics:`
	`Link DOWN`

SH SERVEr CO	Shows server network statistics
	Sample output:
	`Seconds Since Zeroed: 163     Frames Sent,1 Collision: 26`
	`Bytes Received:72950         Frames Sent, 2+Collision: 5`
	`Bytes Sent:18726             Send Failures: 0`
	`Frames Received:752          Send Failure Reasons: 0`
	`Frames Sent: 181             Receive Failures:   503`
	`Multicast Bytes Rcv'd:64474   Receive Failure Reasons: 1`
	`Multicast Bytes Sent: 2406    Unrecognized Destination: 0`
	`Multicast Frames Rcv'd:626    Data Overrun: 0`
	`Multicast Frames Sent:11      User Buffer Unavailable:0`
	`Frames Sent, Deferred:2014    System Buffer Unavailable:1`

Command	Description

SH VErsion	Shows firmware version of print server
	Protocols supported: NetBIOS SNMP TCP/IP EMail DHCP
	Sample output:
	`serial server`
	`Firmware Ver. 4.19 (2004.10.31)`
	`Boot Ver. 1.4`
	`16Mbit Flash`

ZEROKEYS	Overwrite stored cryptographic keys and CSPs

Service Commands

Table 14 Service Commands

Command	Description
SET SERVI <service name> BOT	Sets beginning of transmission (BOT) string index for service The SH SERVI STRings command displays the available strings and their associated number; the default value is 1. Format: `SET SERVI <service name> BOT   nn`
SET SERVI <service name> EOT	Sets end of transmission (EOT) string index for service The SH SERVI STRings command displays the available strings and their associated number; the default value is 1. Format: `SET SERVI <service name> EOT  nn`
SH SERVI STRings [*string_num*]	Displays the BOT and EOT strings used in services If *string_num* is provided, then the specific string definition and expansion display. If *string_num* is not provided, then all string definitions display without their expansions. Sample Output: `10: \FF\04\FF\05\FF\06\FF\08`
SET SERVI <service name> FIlter	Sets filter index for service Format: `SET SERVI <service name> FIlter  nn`
SH SERVI FILters	Shows filter settings Sample output:

Command	Description

	`#  Service Name          Filter`
	`1 TWC_FFFFFF           0: No Filter`
	`2 BINARY_P1            0: No Filter`
	`3 TEXT_P1              1: Text Substitution m= LF, r= CRLF`
	`4 TWC_FFFFFF_P1_4      0: No Filter`
	`5 TWC_FFFFFF_P1_5      0: No Filter`
	`6 TWC_FFFFFF_P1_AT     4: PostScript Tagged Binary`

SET SERVI <service name> FMS	Sets filter 1 text replacement match string index. If the index is zero, the default string of <LF> (line feed) is used. The default value is 0. Format: `SET SERVI <service name> FRM  nn`
SET SERVI <service name> FRS	Sets filter 1 text replacement replace string index. If the index is zero, the default string of <CRLF> (carriage return-line feed) is used. The default value is 0. Format: `SET SERVI <service name> FRS  nn`
SET SERVI <service name> IP	Enables or disables IP based jobs such as lpd, raw tcp and ftp, on the service The default value is enabled for service 1 and 2, disabled for all others. Format: `SET SERVI <service name> IP  [ENable | DIsable]`
SET SERVI <service name> NAme	Changes service name The default value varies by service Format: `SET SERVI <service name> NAme  <newname>`
SET SERVI <service name> POrt	Sets output port associated with a service The default value is S1. Format: `SET SERVI <service name> POrt   <portname>`
SET SERVI <service name> PRIority	Sets priority for service for multiple service transmissions simultaneously The default value is 10. Format: `SET SERVI <service name> PRIority nn`
SH SERVI PRI [*service_num*]	Shows priority of service. If *service_num* is not provided, the priority of all services is listed.
SET SERVI <service	Sets receive only mode for a service

Command	Description
name> RECeive	This option is required only for host applications that do not operate properly if data is received from the serial device. The default value is disabled. Sample output: `SET SERVI <service name> RECeive [ENable	DIsable]`
SET SERVI <service name> TCP	Sets raw TCP port for service If port number is 0, raw TCP is disabled on service. The default value is 9100 for service 1, 3001 for service 2. Format: `SET SERVI <service name> TCP  nn`
SH SERVI SUMmary [*service_num*]	Shows the basic parameters for a specific service. If *service*_num is not provided, parameters for all services are displayed. The command SH SERVI displays the same data as SHOW SERVI SUM.

String Commands

Table 15 String Commands

Command	Description
SET STRing	Set service string table entry String 1 to11 cannot be set or changed. Format: `SET STRing <string #> ”value”`
CL STRing	Clears the service string table entry Format: `CL STRing <string #>`

Command	Description

SH STRing [*string_num*]	Defines the BOT and EOT strings used in services
	If *string_num* is provided, then the specific string definition and expansion are displayed. If *string_num* is not provided, then all string definitions are displayed without their expansions.
	Sample output:
	`1:`
	`2: \1BE`
	`3: \04`
	`4: \1B%-12345X`
	`5: @PJL`
	`6: ENTER LANGUAGE=`
	`7: PCL\0A`
	`8: POSTSCRIPT\0A`
	`9: \FF\04\FF\05\FF\06\FF\07`
	`10: \FF\04\FF\05\FF\06\FF\08`
	`11: \0C`

SH FILters	Shows the filters that can modify a job stream
	Sample output:
	`#    Filter`
	`0    No Filter`
	`1    Text Substitution`
	`2    AppleTalk`
	`3    Text to PostScript`
	`4    PostScript Tagged Binary`
	`5    DC1 Special`

TCP/IP Commands

Table 16 TCP/IP Commands

Command	Description
SET IP ACcess	Allows or prevents access to a block of remote addresses The default value is empty list. Format: `SET IP ACcess [EN | DI | ALL] aa.bb.cc.dd {MAsk ee.ff.gg.hh]`

Command	Description
SET IP RANge	Allows or prevents access to a range of remote addresses The default value is empty list. Format: `SET IP RANge [EN | DI | ALL] aa.bb.cc.dd {MAx ee.ff.gg.hh]`
SH IP ACcess	Displays current access list settings Sample output: `All hosts permitted access`
SET IP ADdress	Sets server IP address The default value is 192.0.0.192 Format: `SET IP ADdress aa.bb.cc.dd`
SET IP ARP ENable	Enables or disables setting of IP address with an ARP packet The default value is Enable. Format: `SET ARP [ENable | DIsable]`
SET IP BAnner	Enables or disables printing of job banner on LPD jobs The default value is Disable. Format: `SET IP BAnner [ENable | DIsable]`
SET IP CHKSUM	Enables or disables verification of IP checksum on received packets The default value is Enable. Format: `SET IP CHKSUM [ENable | DIsable]`
SET IP BOot	Sets number of tries for each enabled IP boot method, if not set to static The default value is 3. Format: `SET IP BOot   n`
SET IP ENable	Enables or disables all IP based protocols The value is Enable. Format: `SET IP [ENable | DIsable]`
SET IP FTIme	Sets IP timeout If enabled, the IP timeout is measured in seconds. If disable, the IP timeout is in minutes. The default value is Disable. Format: `SET IP FTIme    [ENable | DIsable]`

Command	Description
SET IP FTP	Enables or disables FTP protocol The default value is Enable. Format: `SET IP FTP    [ENable | DIsable]`
SET IP HTTP	Enables or disables HTTP protocol The default value is Enable. Format: `SET IP HTTP    [ENable | DIsable]`
SET IP KEepalive	Sets interval in minutes for sending TCP keepalive packets on a connection The default value is 5 minutes. Format: `SET IP KEepalive n`
SET IP LPD	Enables or disables the LPD protocol The default value is Enable. Format: `SET IP LPD    [ENable | DIsable]`
SET IP MEthod	Sets method of getting IP address The default value is Auto. Format: `SET IP MEthod    [ AUTO | BOOTP | RARP | DHCP | STATIC ]`
SET IP PIng	Sends IP ping packets to test connection to remote host Format: `SET IP PIng  aa.bb.cc.dd`
SET IP PRObe	Enables or disables TCP connection probes The default value is Disable. Format: `SET IP PRObe  [ENable | DIsable]`

SET IP RARp	Enables setting of default router and/or subnet mask based on RARP IP address set
	The default value is 0.
	Format:
	`SET IP RARp  nn`
	`nn: 0=both 1=no subnet,  2=no router, 3=neither`

SET IP REtry	Enables or disables LPD retry on incomplete job The default value is Disable. Format: `SET IP REtry  [ENable | DIsable]`

Command	Description
SET IP ROuter	Sets default router address The default value is 0.0.0.0. Format: `SET IP ROuter    aa.bb.cc.dd`
SET IP SUbnet	Sets IP subnet mask The default value is 0.0.0.0. Format: `SET IP SUbnet    aa.bb.cc.dd`
SET IP TCP	Enables or disables the raw TCP 9100 protocol The default value is Enable. Format: `SET IP TCP    [ENable | DIsable]`
SET IP TELnet	Enables or disables Telnet protocol The default value is Enable. Format: `SET IP TELnet [ENable | DIsable]`
SET IP TFTP	Enables or disables TFTP protocol The default value is Enable. Format: `SET IP TFTP   [ENable | DIsable ]`
SET IP TImeout	Sets TCP inactivity timeout. If fast timeout is enabled, the timeout is calculated as seconds. If fast timeout is disabled, the timeout is calculated as minutes. The default value is 1 minute. Format: `SET IP Timeout   n`
SET IP WIndow	Sets TCP maximum window size in bytes The default value is 10240. Format: `SET IP WIndow    nn`

Command	Description
SH IP	Shows TCP/IP related parameters Sample Output:

```
IP is enabled
IP address    192.0.0.192     Boot tries    3
Subnet mask   0.0.0.0         Boot method   AUTO
IP Gateway    0.0.0.0         Max window    10240
 (set manually)
LPD banner    disabled        Timeout         1 min
LPD retries are disabled      Keepalive       5 min

Service                 Port    TCP port
xxxxxx_S1_A              S1       9100
xxxxxx_S1_B              S1       3001
```

Firmware Update

Table 17 Firmware Update

Command	Description
SET LOAd ENable	Sets the firmware to perform a soft reset and enter the server boot program after the next Exit command. This command is used for diagnostic purposes only. The default value is Disable. Format: `SET LOAd (ENable | DIsable ]`
SET LOAd HOst	Sets the node name of the TFTP boot host. This command is used for diagnostic purposes only. The default value is null>\ Format: `SET LOAd HOst      <name>`
SET LOAd IP	Sets source computer IP address for TFTP get operation. The default value is 0.0.0.0. Format: `SET LOAd IP   aa.bb.cc.dd`
SET LOAd SOftware	Sets filename on host for TFTP get update Format: `SET LOAd SOftware  <filename>`
SET LOAd TFTP	Initiates firmware update using TFTP get operation. The TFTP server address must be set using SET LOAd IP and the filename using SET LOAd SOftware. The server will reset after the firmware update is completed. Format: `SET LOAd TFTP`
SET LOAd XModem	Initiates firmware update using the XModem protocol on the serial console The server will reset after the firmware update is completed. Format: `SET LOAd XModem`

SH LOAd	Shows the firmware update parameters
	Sample output:
	`Firmware load is disabled`
	`Load Host IP   = 0.0.0.0`
	`Software file  = xxxx.bin`
	`Load Host Name =`

Miscellaneous Commands

Table 18 Miscellaneous Commands

Command	Description
SET DEFAULT	Set parameters to factory defaults
EXIT	This command exits the current configuration console session.
SH FATal	Shows fatal error log, if fatal errors exist.
CL FATal	Clears the fatal error log
INIT	Instructs the server to execute a soft reset when the next exit command is executed.
SET PAssword	Sets the server access (read) password
SET POWERON	Sets Power on delay
SH POWERON	Displays Power on delay in seconds
SET PROTect	Sets update password to the string given. If set, no configuration values can be changed unless this password has been provided.
CL PROTect	Sets update password to <null>.
SAVE	Saves the current configuration to non-volatile memory. Without this command, the configuration is not saved unless an EXIT command is performed.
SH TEst	Sends the configuration data via ASCII to the serial port
UNPROTECT	If an update password has been defined (SET PROTECT), this command enters the password to allow configuration items to be modified. After entering this command, the server will prompt for the update password. If entered properly, the user will then be able to execute SET commands to modify the server configuration. This lasts only until the console session is terminated with an EXIT command.

Help Commands

For help, simply enter HELP preceding the command. The correct syntax and a brief description of the commands will display. For example, when inquiring for various commands to display specific IP parameters, type HELP SHOW IP, or for commands to change specific wireless/network security parameters, type HELP SET NWRK.

Appendix C
Firmware Update Procedures

Occasionally it may be necessary to update the Serial Device Server to take advantage of new features or to fix specific problems. The simplest way to perform this update is with the Silex UpdateIP utility for Windows XP and 2000 computers. This utility can be found on the CD-ROM that is included with the Serial Device Server, or it can be downloaded from the *Support & Downloads* section of the Silex website (www.silexamerica.com).

When updating the firmware, it is important that power not be removed from the module until the update operation is complete. Power interruption during firmware update can corrupt the firmware image and render the device unusable. The Cryptographic Officer should be sure the update has completed and the unit has reset and returned to normal operation before removing power from the unit.

To use UpdateIP:

1. Download the appropriate firmware update file from *the Support & Download* section of the Silex website (www.silexamerica.com) into a directory on your computer.
2. Download or copy the UpdateIP software files into a directory on your computer.
3. Double click the updateip.exe icon to start the UpdateIP application.
4. Click ***OK*** when you get the ***About Update for TCP/IP*** splash screen

> **Important:** Make sure that the UpdateIP application is included as an exception if you have a firewall enabled on your PC.

on this screen. Click ***OK.***

7. The program will search the local network for Serial Device Servers. Click ***OK*** when the search process is complete.
8. A list of available Serial Device Servers will appear. Highlight the Serial Device Server(s) that you wish to update.
9. From the menu bar, select ***Update*** and then ***Start*** to update the Serial Device Server(s).

If you cannot use UpdateIP, you can use the trivial file transfer protocol (tftp) to update the Serial Device Server firmware:

1. Download the appropriate firmware update file from the *Support & Downloads* Section of the Silex website (www.silexamerica.com) into a directory on your computer.
2. If you are using Windows 2000, XP, or Vista, enter the following command from the command line of your operating system:

```
tftp  -i ipaddress  put  filename  <password>
```

where *ipaddress* is the IP address of the Serial Device Server, *filename* is the file name (and path, if necessary), and <password> is the Serial Device Server password (if you changed this password, use your new password instead of “access”). For example, to download the file tathsti130.bin from the updates directory on your computer into a Serial Device Server with an IP address of 192.168.5.70, you would enter the command:

```
tftp  -i 192.168.5.70  put  /updates/tathsti130.bin  access
```

If you are using a different operating system, please refer to the documentation of that operating system for information on how to use the tftp command. Note that you should specify that the tftp destination file is the Serial Device Server password (“access” by default).

Appendix D
Safety and Regulatory Notices

Information for United States Users

This equipment has been tested and found to comply within the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio and television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver,
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

The user is cautioned that changes and modifications made to the equipment without the approval of manufacturer could void the user's authority to operate this equipment.

Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

The radiated output power of the print server is far below the FCC radio frequency exposure limits. Nevertheless, print server shall be used in such a manner that the potential for human contact during normal operation is minimized.

To satisfy RF exposure requirements, this device (SX-500) and its antenna(s) must operate with a separation distance of at least 20 centimeters from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users must be provided with specific operating instructions for satisfying RF exposure compliance.

Declaration of Conformity (FCC) (SX-500)

According to 47CFR, Part 2 and 15 for Class B Personal Computers and Peripherals; and/or CPU Boards and Power Supplies used with Class B Personal Computers:

We:	Silex Technology America, Inc.
Located at:	157 West 7065 South Salt Lake City, UT 84047, USA

Declare under sole responsibility that the product identified herein, complies with 47CFR Part 2 and 15 of the FCC rules as a Class B digital device FOR HOME OR OFFICE USE. Each product marketed, is identical to the representative unit tested and found to be compliant with the standards. Records maintained continue to reflect the equipment being produced can be expected to be within the variation accepted, due to quantity production and testing on a statistical basis as required by 47CFR §2.909. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Trade Name:	silex
Type of Product:	Ethernet and Wireless 802.11b and 802.11g-enabled serial server
Model:	SX-500

Silex Technology America, Inc. hereby declares that the equipment specified above conforms to the above requirements.

Standards used and met in the assessment:

- CFR Title 47, Part 15, Subpart B and Subpart C; EN55022: 1998 Class B
- FCC ID: N6C-SX10WG

Information for Canadian Users (IC notice) (SX-500)

The term “IC” before the radio certification number only signifies that Industry of Canada technical specifications were met. Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations (RSS-210, IC: 4908A-SX10WG).

To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment that is installed outdoors is subject to licensing.

This device has been designed to operate with an antenna having a maximum gain of 2 dB. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen than the equivalent isotropically radiated power (EIRP) is not more than the required for successful communication.

Information for European Users (SX-500)

The server and its built-in 802.11b, and 802.11g wireless technology is in compliance with the Class B Information Technology Equipment requirements and other relevant provisions of European Directive 1999/5/EC. The limits for Class B equipment were derived for typical residential environments to provide reasonable protection against interference with licensed communications devices. The internal function is a radio device using the 2.4 GHz frequency band (2.400GHz - 2.4845 GHz). It is intended for wireless communication with other 802.11b, and 802.11g-enabled devices in an indoor environment.

The use of 802.11b and 802.11g wireless technology in certain countries may be restricted. Before using 802.11x products, please confirm with the frequency management authority in the country where you plan to use it. Many countries allow indoor use only. In Italy, general authorization is required if used outside. In France, the use of certain channels is restricted outdoors. In some situations or environments, the use of 802.11x wireless technology might be restricted by the proprietor of the building or responsible representatives of the organization, for example, in airplanes, in hospitals or in any other environment where the risk of interference with other devices or services is perceived or identified as harmful.

If you are uncertain of the policy that applies to the use in a specific organization or environment, you are encouraged to ask for authorization to use 802.11x wireless technology prior to switching it on. Consult your physician or the manufacturer of personal medical devices (pacemakers, hearing aids, etc.) regarding any restrictions on the use of 802.11x wireless technology.

Silex cannot be responsible for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product.

Declaration of Conformity (CE) (SX-500)

Manufacturer: Silex Technology America, Inc.
157 West 7065 South
Salt Lake City, UT 84047, USA
Telephone: (801) 748-1199

Product: Ethernet and Wireless 802.11b and 802.11g-enabled serial server
Model No.: SX-500

Silex Technology America, Inc. hereby declares that the above-referenced product, to which this declaration relates, in is conformity with the provisions of:

Council Directives 1999/5/EC, Radio Equipment and Telecommunications Terminal Equipment.

Standards used and met in the assessment:

- EN301 489-1
- EN301 489-17
- EN300 328

The documents required by this Directive are maintained at the corporate headquarters of Silex Technology America, Inc., 157 West 7065 South, Salt Lake City, UT 84047, USA

Appendix E
Silex Contact Information

Silex Technology America, Inc.
www.silexamerica.com
Technical Support: support@silexamerica.com
Sales: sales@silexamerica.com
Tel: (801) 748-1199 8:00 to 5:00 Mountain Time
Tel: (866) 765-8761 toll-free
Fax: (801) 748-0730

Silex Technology Europe GmbH
www.silexeurope.com
Tel: +49-2159-67500
Tel: 0800-7453938 German toll free
Email: contact@silexeurope.com

Silex Technology Beijing, Inc.
www.silex.com.cn
Tel: +86-10-8497-1430
Email: contact@silex.com.cn

Corporate Headquarters
Silex Technology, Inc.
www.silex.jp
Tel: +81-6-6730-3751
Email: support@silex.jp

silex
technology

Silex Technology America, Inc.

www.silexamerica.com